

LANDesk® Management Suite 8.6

User's Guide



»»
LANDesk®



Nothing in this document constitutes a guaranty, warranty, or license, express or implied. LANDesk disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of LANDesk; indemnity; and all others. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of LANDesk.

LANDesk retains the right to make changes to this document or related product specifications and descriptions at any time, without notice. LANDesk makes no warranty for the use of this document and assume no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright © 2004-2005, LANDesk Software Ltd. or its affiliated companies. All rights reserved.

LANDesk is either a registered trademark or trademark of LANDesk Software, Ltd. or its controlled subsidiaries in the United States and/or other countries.

*Other brands and names are the property of their respective owners.

Table Of Contents

Table Of Contents.....	iii
Introduction to LANDesk Management Suite 8	13
What's new in LANDesk Management Suite 8	14
What you can do with Management Suite 8	18
Where to go for more information	19
Starting the console	21
Activating the core server	22
Starting the console.....	25
Changing the core server connection	26
Using the console	27
Console overview	28
Understanding the network view	29
Creating groups.....	32
Device icons	33
Viewing managed devices in the All Devices group	34
Shortcut menus	35
Configuring the network view with column sets	37
Toolbar options.....	40
Using console tools	41
Dockable tool windows.....	42
Saving window layouts	43
Find bar	44
Status bar	45
Viewing device properties	46
Monitoring devices for network connectivity	49
Working with devices that support Intel® AMT	50
Using role-based administration.....	55
Role-based administration overview	56
Managing LANDesk users	58
Managing groups.....	61
Understanding rights	63
Creating scopes	69
Assigning rights and scope to users	72
Configuring services	73

TABLE OF CONTENTS

Selecting a core server and database with General settings.....	74
Configuring the Inventory service.....	75
Configuring the scheduler service.....	78
Configuring the custom jobs service	80
Configuring the Multicast service	82
Configuring the OS deployment service.....	83
Configuring device agents	85
Working with agent configurations	86
Agent security and trusted certificates	90
Uninstalling device agents	93
Using LANDesk Server Manager and LANDesk System Manager with LANDesk Management Suite	94
Installing Linux server agents.....	95
Using database queries.....	103
Queries overview.....	104
Query groups.....	105
Creating database queries	106
Running database queries	108
Importing and exporting queries.....	109
Using LDAP queries	111
About the Directory manager window	112
More about the Lightweight Directory Access Protocol (LDAP)	115
Managing inventory	117
Inventory scanning overview.....	118
Viewing inventory data	120
Tracking inventory changes	122
Using custom data forms	123
Using reports	127
Reports overview.....	128
Running and viewing reports.....	130
Publishing reports.....	131
Creating custom reports.....	135
Importing and exporting reports	140
Creating .CSV files	141
Using scripts and tasks.....	143
Managing scripts	144
Scheduling tasks	145

Using the default scripts	150
Configuring local scheduler scripts	151
Using remote control	153
Using the remote control viewer.....	154
Changing device remote control security	159
Using remote control logging	160
Customizing the viewer and remote control agents	161
Troubleshooting remote control sessions	164
Using software distribution	165
Software distribution overview	166
Setting up the delivery server.....	170
Distributing a package.....	173
Distributing software to Linux devices.....	179
Troubleshooting distribution failures	180
Using policy-based distributions.....	181
About policy-based management.....	182
Configuring policies	184
Building packages	187
Setting up a package-building computer.....	188
Package-building overview	189
Running the Package Builder wizard	191
Uninstalling software distribution packages	192
Using software license monitoring.....	195
Monitoring software license compliance	197
Creating product and vendor aliases	206
Editing software inventory	208
Exporting and importing software license monitoring data	211
Using unmanaged device discovery.....	215
Discovering unmanaged devices	216
Using OS deployment.....	221
OS deployment overview	222
OS image guidelines	223
Customizing images with Setup Manager and Sysprep	225
Agent-based deployment	227
Creating imaging scripts with the OS Deployment/Migration Tasks wizard.....	228
Modifying scripts.....	230
Multicasting OS images.....	231

TABLE OF CONTENTS

Viewing image status reports	233
PXE-based deployment	234
Using PXE representatives	235
Booting devices with PXE	237
Understanding the PXE boot options	238
Using profile migration.....	243
Profile migration overview	244
Profile content	246
Creating migration scripts with the OS Deployment/Migration Tasks wizard	251
Creating user-initiated profile migration packages	253
Running user-initiated profile migration packages	254
Using the Web console.....	255
Overview	255
About the Web console	255
The console	257
Starting the console.....	257
Using the console.....	258
Targeting devices	263
Filtering the display list.....	264
Using groups	265
Custom columns.....	267
Custom attributes	268
Page settings.....	269
Role-based administration	270
About role-based administration	270
Adding product users	276
Creating scopes	278
Assigning rights and scope to users	280
Remote server access.....	282
About remote access.....	282
Controlling remote Windows devices	284
Accessing remote Linux devices	288
Software distribution.....	289
Software distribution overview	289
Distribution file descriptions	295
About Distribution packages	297
About the Scheduled tasks tab	299

About the Delivery methods tab	300
Understanding distribution error codes	302
Troubleshooting distribution failures	304
Scripting overview	306
Running the Package Builder wizard	311
Setting up a package-building computer.....	312
Building a package	313
Scripts	316
Managing scripts	316
Using the default scripts	318
Scheduling tasks	319
Reports.....	322
About reports.....	322
Viewing reports.....	323
Queries	324
Using queries	324
Understanding custom queries	328
Creating custom queries	329
Step 1: Creating a search condition (required)	330
Step 2: Selecting attributes to display (required)	331
Step 3: Sorting results by attribute (optional).....	332
Step 4: Running the query	333
Viewing query results	334
Viewing drill-down query results.....	335
Exporting query results to CSV files.....	336
Changing query column headings.....	337
Exporting and importing queries	338
About the Directory manager window	340
Creating LDAP directory queries.....	341
More about the Lightweight Directory Access Protocol (LDAP)	343
Inventory management.....	344
Managing inventory	344
Inventory scanning overview	345
Viewing inventory data	347
Editing the LDAPPL3.TEMPLATE file.....	349
Software licenses	351
Monitoring software license compliance	351

TABLE OF CONTENTS

Publishing the application list	359
Using Asset Manager	360
Asset Manager overview	362
Accessing Asset Manager in the Web console	365
Managing assets	366
Working with computer assets	368
Working with software assets.....	371
Managing contracts	373
Managing invoices.....	374
Managing projects	375
Managing global lists.....	376
Creating new types.....	378
Using a details summary	380
Adding details.....	382
Adding detail tables	386
Managing detail templates	387
Adding detail templates	388
Using an item list	389
Adding items to the database.....	390
Associating items	392
Importing items	393
Exporting items.....	395
Using Asset Manager reports.....	397
Core database installation and maintenance	400
Using rollup databases	400
Configuring rollup database links	403
Multi-core support.....	408
Troubleshooting tips	410
Managing local accounts	415
Local accounts overview	416
Using the file replicator	421
Using the file replicator.....	422
Managing Macintosh devices	425
LANDesk for Macintosh overview	426
Tools for Macintosh.....	427
Agent Configuration for Macintosh devices	429
Inventory for Macintosh devices.....	434

Software Distribution for Macintosh devices	435
Managed scripts for Macintosh devices	438
Remote control for Macintosh devices	439
Operating system deployment for Macintosh devices	440
Reporting for Macintosh devices	442
Scheduled tasks for Macintosh devices	443
Software license monitoring for Macintosh devices	444
Security and Patch Manager for Macintosh devices	445
Managing a client Macintosh machine	446
Using Security and Patch Manager	449
Security and Patch Manager overview	451
Understanding and using the Security and Patch Manager window	455
Security and patch management workflow	461
Configuring devices for security scanning and remediation	462
Updating security and patch content	466
Viewing security and patch content	469
Purging unused definitions	471
Creating custom definitions and detection rules	472
Downloading patches	477
Uninstalling patches	478
Scanning devices (for each security content type)	480
Remediating devices	484
Remediation methods	488
Viewing security and patch information for scanned devices	492
Other security management tasks	494
Using LANDesk trusted access	497
LANDesk Trusted Access overview	499
Understanding the two solutions and selecting LANDesk DHCP or Cisco NAC	503
Setting up and configuring a remediation server	533
Configuring the LANDesk DHCP server	539
Using connection control manager	559
Using connection control configurations to restrict network access	560
Using device control configurations to restrict USB device access	562
Configuring alerts	568
Deploying configurations	569
Using alerts	571
How alerting works	572

TABLE OF CONTENTS

Configuring AMS alert actions.....	573
Working with configured alert actions	580
Viewing the AMS Alert History	582
Using the Asset Manager add-on.....	585
Asset Manager overview	587
Accessing Asset Manager in the Web console	590
Managing assets	591
Working with computer assets	593
Working with software assets.....	596
Managing contracts.....	598
Managing invoices.....	599
Managing projects	600
Managing global lists.....	601
Creating new types.....	603
Using a details summary	605
Adding details.....	607
Adding detail tables	611
Managing detail templates	612
Adding detail templates	613
Using an item list	614
Adding items to the database.....	615
Using asset alert dates.....	617
Associating items	620
Importing items.....	621
Exporting items.....	623
Using Asset Manager reports.....	625
Using Handheld Manager.....	629
Installing Handheld Manager	630
Using Handheld Manager	632
Transferring files to and from Pocket PC handhelds	635
Working with BlackBerry devices	637
Using LANDesk Inventory Manager	639
Appendix A: Additional inventory operations and troubleshooting	641
Scanning custom information.....	642
Specifying the software scanning interval and history	643
Appendix B: Additional OS deployment and profile migration information.....	651
Additional OS deployment procedures.....	652

Using the LANDesk imaging tool for DOS	658
Using the LANDesk imaging tool for Windows	661
Appendix C: Additional software distribution information	665
Scripting guide for .CFG files	666
Processing custom scripts	671
Troubleshooting .CFG files and their packages.....	674
Scripting guide for deployment scripts (.INI files).....	676
Understanding software distribution error codes	678
Files used in script-based software distribution	681
Appendix D: Additional security scanner information	683
Context-sensitive help	687
Activating the core server.....	688
Starting the console.....	691
Changing the core server connection	692
Role-based administration help.....	693
Managed device help	695
Inventory help.....	708
Reports help	713
Unmanaged Device Discovery help	716
Scheduled tasks help	718
Using the Distribution package dialog.....	721
Using the Delivery methods dialog.....	725
Distributing files with a file transfer script.....	732
OS deployment and Profile migration wizard help	733
Software license monitoring help	747
Handheld Manager help	752
Security and Patch Manager help	753
Macintosh help	774
Configuring the LANDesk Management Gateway	775
Local accounts management help	777

Introduction to LANDesk Management Suite 8

LANDesk® Management Suite 8 consists of tools you can use to help manage your Windows*, NetWare*, Macintosh*, Linux*, and UNIX* devices. Use these tools to distribute software packages, monitor software usage, deploy OS images and migrate profiles, remote control devices, and complete many other management tasks.

In this chapter, you'll learn more about Management Suite 8, including:

- What's new in this release
- What you can do with Management Suite 8
- Where to go for more information

What's new in LANDesk Management Suite 8

LANDesk Management Suite 8, version 8.6 adds these enhancements:

- **New LANDesk Trusted Access tool:** Adds endpoint compliance security to your network. Lets you configure custom compliance security policies using the Security and Patch Manager tool, and enforces those policies on devices attempting to access your network through a posture validation process. Healthy devices are granted access while unhealthy devices are quarantined, where they can be remediated and granted full access or given limited network access. Trusted access requires additional hardware and software setup and a strong practical knowledge of network routing and DHCP services. LANDesk offers two trusted access solutions: a Cisco NAC integrated solution, and a LANDesk DHCP server-based solution.
- **Enhanced Security and Patch Manager:** New enhancements to the Security and Patch Manager tool include: real-time spyware detection and removal, frequent security scanning for high-risk threats, antivirus support via scanner and pattern file checking, firewall state detection and configuration, configurable security threat definitions through custom variables, vulnerability supercedence and dependencies notification, security scanning by custom groups, ability to divide scheduled repair jobs into staging and deployment tasks, custom alerting, new reports, additional security content types, additional supported languages, and more.
- **New LANDesk Management Gateway:** The Management Gateway lets you manage users that are outside of your corporation, without putting holes in your firewall. Includes support for remote control, software distribution, inventory, software license monitoring, and more.
- **Improved software distribution:** Support for Linux RPM software distribution. Task targeting has been improved so you can target combinations of queries, device groups, and specific devices. Management Suite automatically resolves duplicates so the same device won't get the job multiple times if it's targeted more than once.
- **Improved Remote control:** Improved keyboard mapping, so special characters that you type locally appear on the target device correctly. Improved remote screen blanking is now part of the mirror driver. Other applications won't override the screen blanking once it's enabled. Remote controlling devices running older agent versions now works better from the Web console.
- **Improved connection control manager:** Includes more granular control of USB devices, including the ability to create custom rulesets. Supports Bluetooth* restrictions.
- **New report engine:** Integration of Active Reports for producing reports (Crystal reports is no longer supported).
- **Enhanced reports tool:** Additional predefined reports provided. Create custom report templates with the report designer. Added a charting tool to provide a graphical representation of the data. Schedule reports to be published and e-mailed to recipients. See Using reports.
- **New local accounts management:** An administrative tool used to manage the users and groups on local machines on your network. From the console, you can add and delete users and groups, add and remove users from groups, set and change passwords, edit user and group settings, and create tasks on devices. See Managing local accounts.
- **New OSD for Macintosh:** The operating system deployment (OSD) feature is used to deploy OS images to Macintosh devices. This method uses a device's existing OS and installed LANDesk agents to deploy the images. See Operating system deployment for Macintosh devices.

LANDesk Management Suite 8, version 8.5 adds these enhancements:

- **Improved software distribution:** Redesigned software distribution interface makes it much easier to create distribution packages and package delivery methods. Package chaining enables administrators to define package dependencies and automatically install prerequisite software packages. Expanded task status reporting provides greater insight into deployment status, successes, and failures. See *Using software distribution*.
- **Redesigned and expanded Security and Patch Manager tool:** This tool is now installed by default with Management Suite to let you scan managed devices, as well as core servers and console machines, for LANDesk software updates. You can also create your own custom security definitions to scan devices for specific, potentially threatening conditions. In order to take full advantage of the tool's security scanning and remediation capabilities (including protection from known vulnerabilities for Windows, Macintosh, and Linux; spyware; Windows configuration security threats; and more), you must purchase a separate LANDesk Security Suite content subscription. With the appropriate subscription, you can download the latest known vulnerability definitions and required patches and use them to create and run custom security scan and remediation tasks, all from the Management Suite console. Configure whether the security scanner displays on end user devices during scan and repair processes, device reboot options, and the level of user interaction. You can also view comprehensive security and patch information for scanned devices. See *Using the Security and Patch Manager tool*.
- **New Connection Control Manager tool:** Monitors and restricts access to managed devices through network connections and I/O devices. You can restrict the network IP addresses that devices are allowed to connect with, and you can also restrict the use of devices that allow data access to the device, such as ports, modems, drives, USB ports, and wireless connections. See *Using connection control manager*.
- **Improved remote control:** Application layer remote control provides greater stability and improved performance. New remote control viewer is easier to use, offers "view only" support, and provides screen draw tools for remote training and problem resolution. See *Administering remotely*.
- **New report publishing:** Report publishing capabilities enable you to schedule and automatically generate reports in .HTML, .PDF, .DOC, .RTF and .XLS formats, and publish those reports to a secure file share where they can be viewed by anyone to whom you've provided the required access credentials. See *Using reports*.
- **Enhanced inventory:** The inventory scanner now supports SMBIOS 2.1 and above, and provides greater detail, including memory and expansion slot data, network adaptor settings, drive information, and plug-and-play monitor details.
- **Improved software license monitoring:** Expanded software license monitoring features include predefined applications list and compliance tracking by group, department, and organizational unit. See *Using software license monitoring*.
- **New software portal:** Gives users self-service access to policy-based application packages from their own desktop. See *Using the local software distribution portal*.
- **New LANDesk file replicator:** Allows you to easily replicate data hosted on Web servers. See *Using the file replicator*.

LANDesk Management Suite 8, version 8.1 adds these enhancements:

- **Enhanced inventory:** Launch an immediate inventory scan on a device by right-clicking the device and clicking **Inventory**. Also, the inventory scanner now collects the operating system language on devices.
- **Improved software distribution:** Software distribution now works better through firewalls, and you can now disable task completion on software distribution jobs, so if the job fails it isn't automatically retried.

- **Improved Web console:** Use software license monitoring from the Web. See Monitoring software license compliance.
- **Enhanced application policy management reliability:** Whenever a device checks with the core server for tasks or policies, the core server updates that device's IP address in the core database, avoiding problems with outdated IP addresses that may be part of an old inventory scan.
- **Improved scheduled task support:** Provide multiple logins for the scheduler service to authenticate with when running tasks on devices that don't have Management Suite agents. This is especially useful for managing devices in multiple Windows domains. See Configuring the scheduler service.
- **New custom local scheduler tasks:** Use the Management Suite local scheduler on devices to remotely schedule a recurring task. See Configuring local scheduler scripts.
- **Enhanced remote control:** Store detailed remote control logs in the database. Log information includes who initiated the remote control session and the remote control tasks (file transfers, chat, and so on) they did on the device. Also, remote control sessions now pass 3rd mouse button/wheel movement to devices. See Using remote control logging.
- **Enhanced unmanaged device discovery:** Generate reports on the unmanaged devices on your network. For more flexibility, you can now use an Unmanaged Device Discovery task to rediscover managed devices. This is useful if you've reset your database. See Restoring client records.
- **New LANDesk Asset Manager 8 Add-on:** Record and keep track of your critical IT assets such as hardware, software, office equipment, and other physical assets, in addition to invoices, lease agreements, and other associated business documents and information. Create and use customized data entry forms to add items to the database. Reconcile the existence and location of IT assets with financial records. See Using the Asset Manager add-on.
- **Improved Patch Manager 8 Add-on:** You can now create custom vulnerability definitions to check for security risks before a patch is available. Also, scan for vulnerabilities on Mac OS X and Sun Solaris devices. See Using the Security and Patch Manager tool.

LANDesk Management Suite 8, version 8.0 adds these enhancements:

- **Improved database:** New single database schema with improved data integrity and scalability.
- **Role-based administration:** Add Management Suite users and configure their access to Management Suite tools and managed devices based on their administrative role in your network. With role-based administration, you assign scope to determine the devices a user can view and manage, and rights to determine the tasks they can perform. See Role-based administration.
- **Software Distribution improvements:** Enhancements include byte-level checkpoint restart for interrupted downloads, peer download, dynamic bandwidth throttling that limits distribution bandwidth when devices need network bandwidth, and multi-file MSI multicast package support. See Using Targeted Multicasting with software distribution" and "About byte-level checkpoint restart and dynamic bandwidth throttling.
- **New Unmanaged Device Discovery feature:** Discover unknown and unmanaged devices on your network through a directory service, domain discovery, or layer 3 ping sweep. Alerts notify you of newly discovered devices. Schedule device discovery so you can constantly be aware of new devices. See Using Unmanaged Device Discovery.
- **Enhanced device security:** Certificate-based model allows devices to only communicate with authorized core servers and consoles. See Agent security and trusted certificates.

- **New on-demand remote control:** Optional and highly secure on-demand remote control model only loads the remote control agent on devices for the duration of an authorized remote control. See Deploying remote control.
- **New reports:** Over 50 new predefined Management Suite service reports for planning and strategic analysis. See Managing inventory and reports.
- **New console interface:** New console design with dockable tool windows, network view, custom layouts, and more. See Using the LANDesk Management Suite console.
- **Additional Macintosh computer feature support:** Targeted Multicast, Application Policy Management, and Software License Monitoring for Mac OS* X devices. See Managing Macintosh devices.

What you can do with Management Suite

8

With Management Suite 8, you can:

- Use the LANDesk Management Suite console to configure and manage your network. See [Using the LANDesk Management Suite console](#).
- Create and manage queries on inventory data and LDAP directories. See [Using queries](#).
- Manage inventories, track inventory changes, create forms to gather custom data from devices, and view detailed reports. See [Managing inventory](#) and [Using reports](#).
- Diagnose and troubleshoot problems on remote devices from the console. You can remote control, reboot, execute files, and transfer files to devices. See [Administering remotely](#).
- Quickly distribute software to all of your network users. See [Using software distribution](#).
- Use a Web-based console to access key Management Suite features from anywhere you have a browser. See [Using the Web console](#).
- Monitor software licenses and compliance, and track software usage and denial trends. Also edit the core database's software list, LDAPPL3.INI, that the inventory scanner uses to identify device applications. See [Using software license monitoring](#).
- Deploy OS images and migrate user profiles. See [Using OS deployment](#) and [Using profile migration](#).
- Create application policies based on core database queries. Devices targeted by policies automatically receive application sets. See [Using policy-based distributions](#).
- Set up alert actions to notify you when critical thresholds are exceeded (for example, receive an e-mail message if disk usage exceeds 90 percent). See [Using alerts](#).

Where to go for more information

Refer to the *LANDesk Management Suite Installation and Deployment Guide* for:

- Finding out system requirements
- Installing Management Suite
- Activating the core server
- Upgrading from previous versions of Management Suite
- Installing LANDesk add-on products

Using this guide

The *User's Guide* is available as a compiled Windows HTML Help file and as an Adobe Acrobat* PDF file.

- The HTML Help version is available from the console by pressing F1 or by clicking **Help | LANDesk Help**.
- The PDF version is available from your LANDesk installation image in the Docs folder.

If you're using the HTML Help version, you can use the Help window's Search tab to look for topics containing keywords you enter. When you are in a topic, you can search for specific occurrences of a word by clicking in the topic window, pressing **CTRL+F**, and entering the word you want to find.

You can download translated versions of this documentation from <http://www.landesk.com/Support/Downloads/Index.aspx>.

Nothing in this document constitutes a guaranty, warranty, or license, express or implied. LANDesk disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of LANDesk; indemnity; and all others. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of LANDesk.

LANDesk retains the right to make changes to this document or related product specifications and descriptions at any time, without notice. LANDesk makes no warranty for the use of this document and assume no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright © 2004-2005 LANDesk Software, Ltd. or its affiliated companies. All rights reserved. LANDesk is either a registered trademark or trademark of LANDesk Software, Ltd. or its affiliated companies in the United States and/or other countries.

*Other brands and names are the property of their respective owners.

Starting the console

This chapter provides information about activating your core server with a valid LANDesk software license, and starting the console to access and utilize all of the LANDesk tools.

Read this chapter to learn about:

- Activating the core server
- Starting the console
- Changing the core server connection

Activating the core server

LANDesk uses a central licensing server to help you manage your core server's product and node licenses. To use LANDesk products, you must obtain a user name and password that will activate the core server with an authorized certificate. Activation is required on each core server before you can use LANDesk products on that server. You can activate each core server either automatically through the Internet or manually by e-mail. You may need to reactivate a core server in the event that you significantly modify its hardware configuration.

On a periodic basis, the activation component on each core server will generate data regarding:

- The precise number of nodes you're using
- The non-personal encrypted hardware configuration
- The specific LANDesk programs you're using (collectively, the "node" count data)

No other data is collected or generated by the activation. The hardware key code is generated on the core server using non-personal hardware configuration factors, such as the size of the hard drive, the processing speed of the computer, and so on. The hardware key code is sent to LANDesk in an encrypted format, and the private key for the encryption resides only on the core server. The hardware key code is then used to create a portion of the authorized certificate.

After installing a core server, use the Core Server Activation utility (**Start | All Programs | LANDesk | Core Server Activation**) to either activate it with a LANDesk account associated with the licenses you've purchased or with a 45-day evaluation license. The 45-day evaluation license is for 100 nodes. There are two types of licenses, device and server. Any time you install LANDesk agents on a server operating system, such as Windows 2000 Server or Windows 2003 Server, that installation consumes a license for a server. Rollup core servers don't need to be activated.

You can switch from a 45-day evaluation to a paid license at any time by running the Core Server Activation utility and entering your LANDesk username and password.

Each time the node count data is generated by the activation software on a core server, you need to send the node count data to LANDesk, either automatically by the Internet or manually by e-mail. If you fail to provide node count data within a 30-day grace period after the initial node count verification attempt, the core server may become inoperative until you provide LANDesk with the node count data. Once you send the node count data, LANDesk will provide you with an authorized certificate that will allow the core server to work normally once again.

Once you've activated a core server, use the product licensing dialog (**Configure | Product licensing**) to view the products and the number of authorized nodes purchased for the account the core server authenticates with. You can also see the date the core server will verify node count data with the central licensing server. The core server doesn't limit you to the number of authorized nodes you purchased.

About the Core Server Activation utility

Use the Core Server Activation utility to:

- Activate a new server for the first time
- Update an existing core server or switch from a trial-use license to a full-use license
- Activate a new server with a 45-day trial-use license

Start the utility by clicking **Start | All Programs | LANDesk | Core Server Activation**. If your core server doesn't have an Internet connection, see Manually activating a core or verifying the node count data later in this section.

Each core server must have a unique authorized certificate. Multiple core servers can't share the same authorization certificate, though they can verify node counts to the same LANDesk account.

Periodically, the core server generates node count verification information in the "\Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk licensing server. This file is in XML format and is digitally signed and encrypted. Any changes manually made to this file will invalidate the contents and the next usage report to the LANDesk licensing server.

The core communicates with the LANDesk licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Note that the Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.

If your core server doesn't have an Internet connection, you can verify and send the node count manually, as described later in this section.

Activating a server with a LANDesk account

Before you can activate a new server with a full-use license, you must have an account set up with LANDesk that licenses you for the LANDesk products and number of nodes you purchased. You will need the account information (contact name and password) to activate your server. If you don't have this information, contact your LANDesk sales representative.

To activate a server

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use.
4. Click **Activate**.

Activating a server with a trial-use license

The 45-day trial-use license activates your server with the LANDesk licensing server. Once the 45-day evaluation period expires, you won't be able to log in to the core server, and it will stop accepting inventory scans, but you won't lose any existing data in the software or database. During or after the 45-day trial use license, you can rerun the Core Server Activation utility and switch to a full activation that uses a LANDesk account. If the trial-use license has expired, switching to a full-use license will reactivate the core.

To activate a 45-day evaluation

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core for a 45-day evaluation**.
3. Click **Activate**.

Updating an existing account

The update option sends usage information to the LANDesk licensing server. Usage data is sent automatically if you have an Internet connection, so you normally shouldn't need to use this option to send node count verification. You can also use this option to change the LANDesk account the core server belongs to. This option can also change a core server from a trial-use license to a full-use license.

To update an existing account

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Update this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use. If you enter a name and password that's different than the one used to originally activate the core, this switches the core to the new account.
4. Click **Activate**.

Manually activating a core or verifying the node count data

If the core server doesn't have an Internet connection, the Core Server Activation utility won't be able to send node count data. You'll then see a message prompting you to send activation and node count verification data manually through e-mail. E-mail activation is a simple and quick process. When you see the manual activation message on the core, or if you use the Core Server Activation utility and see the manual activation message, follow these steps.

To manually activate a core or verify the node count data

1. When the core prompts you to manually verify the node count data, it creates a data file called {languagecode}-activate.{datestring}.txt in the "%Program Files\LANDesk\Authorization Files" folder. Attach this file to an e-mail message and send it to licensing@landesk.com. The message subject and body don't matter.
2. LANDesk will process the message attachment and reply to the mail address you sent the message from. The LANDesk message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "%Program Files\LANDesk\Authorization Files" folder. The core server immediately processes the file and updates its activation status.

If the manual activation fails or the core can't process the attached activation file, the authorization file you copied is renamed with a .rejected extension and the utility logs an event with more details in the Windows Event Viewer's Application Log.

Starting the console

To start the console

1. Click **Start | Programs | LANDesk | LANDesk Management Suite**. (The actual program name may be different depending on the LANDesk product you've installed and the license used to activate your core server.)
2. Enter a valid user name and password.

If you're connecting to a remote core server, follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

3. Select the core server you want to connect to. The user must have proper authentication credentials to that core server.
4. Click **OK**.

The console opens with the layout (size, position, open tool windows, etc.) that was being used the last time this user logged out.

For additional consoles, the credentials you use to log into Management Suite must match the credentials used for any drives you have mapped to the core server. Otherwise, you might see a "Multiple connections" error in the console login dialog.

If you're running an additional console and have a drive mapped to the core server, you must u

About the Login dialog

Use this dialog to launch the console and connect to a core server.

- **Username:** Identifies a LANDesk user. This might be an administrator user or some other type of user with restricted access (see Using role-based administration). The user must be a member of the LANDesk Management Suite group on the core server. Follow the normal Windows NT rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).
- **Password:** The user's password.

Note: If a LANDesk Administrator changes the password of another user (i.e., an additional console user), the new password does not take affect until that user reboots their console. At that point, the user would enter their new password to log into the console.

- **Core server:** Specifies the core server you want to connect to. This drop-down list is the same as the core server drop-down list available on the console toolbar.

Changing the core server connection

The console lets you view and manage the contents of any database associated with a core server that you can connect to on your network. This allows you to create databases for different sites, organizational units, or logical internal networks.

You can only be connected to one core server at a time.

To change core server connections

1. Select a core server from the **Core** drop-down list located on the console toolbar. Or, enter a core server name in the text box and press **Enter**.

The server is searched for on your network. If found, you're prompted to log in at the standard Login dialog.

2. Enter a valid user name and password.

Follow the normal Windows NT rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

Once you've connected to a core server, its name is automatically added to the **Core** drop-down list in the toolbar.

Using the console

LANDesk Management Suite provides a full range of system management tools that let you view, configure, manage, and protect devices on your network. All of these tasks can be performed via a single console. This chapter introduces the console interface and describes how to configure and navigate the console's network view and tool windows.

Read this chapter to learn about:

- Console overview
- Understanding the network view
 - Creating groups
 - Device icons
 - Viewing managed devices in the All Devices group
 - Shortcut menus
 - Configuring the network view with column sets
 - Toolbar options
- Using console tools
- Dockable windows
- Auto hide
- Saving window layouts
- Find bar
- Status bar
- Viewing device properties
- Configuring agent discovery
- Monitoring devices for network connectivity

Console overview

The power of the console is that you can perform all critical network management functions from one convenient location, freeing you from the need to go to each managed device to perform routine maintenance or to troubleshoot problems. From a single console, you can distribute and update software or configuration settings, diagnose hardware and software issues, deploy OS images and migrate user profiles, use role-based administration to control user access to both features and devices, use remote control features to train end users or resolve problems.

You can have multiple core servers and databases to accommodate your specific network management needs. For information on installing a core server and console, additional consoles, Web console, and managing multiple core servers and databases, refer to the *Installation and Deployment Guide* (this guide is available as a printable PDF document).

Continue reading this chapter to learn how to navigate and use the console to view and organize devices and access the various management tools. (Each tool, such as software distribution, remote control, security and patch Manager, etc, are described in-depth in subsequent chapters in this guide.)

Understanding the network view

The network view is the main window of the console and is the starting point for most functions. This is where you view device's inventory data, create queries to search for and group devices, select devices to remote control, and so on.

The network view window is always open and contains two panes. The left-hand pane shows a hierarchical tree view of the core server/database you're currently connected to and its **Devices**, **Queries**, and **Configuration** groups. You can expand or collapse the tree objects as needed. The right-hand pane in the network view displays a detailed list of the selected group's devices, queries, or configuration items, depending upon which type of group you've selected.

Group icons

The following icons are used to represent different group types in the network view:

- **Blue folder:** Indicates public and private groups.
- **Double yellow folders:** Indicates public groups that contain a comprehensive list of items of a specific type, such as **All Devices**.

You can resize the network view window and its panes and columns, but you can't close it. The network view window is not dockable like the tools windows.

Role-based administration

The devices you can view and manage in the network view, and the management tools you can use, are determined by the access rights and device scope assigned to you by the administrator. For more information, see Role-based administration.

The network view contains the following groups and subgroups:

Core

The **Core** object identifies the core server you're currently connected to. The **Core** object is located directly under the network view root and can be collapsed and expanded.

The syntax for the core object name is: Server Name\Database Instance.

Devices

The **Devices** group contains the following device subgroups.

- **My devices:** Lists devices for the currently logged-in user, based on the user's scope. A user can create device subgroups only under **My devices**. Users can add devices to their **My devices** group, or any of its subgroups, by copying them from the **Public devices** and **All devices** groups. Users can also click and drag devices from **Public devices** and **All devices** into their **My devices** group.

Dragging and dropping items in the network view

When you click an item in order to drag it to another group in the network view, the cursor indicates where you can and can't drop the item. As you move the cursor over a group object, a plus-sign (+) indicates that you can add the item to that group; and a cross-out sign indicates that you can't add the item to that group.

- **Public devices:** Lists devices an administrator (a user with the LANDesk Administrator right) has added from the **All devices** group. An administrator sees all of the devices in this group, while other users see only the devices allowed by their scope. Also, only an administrator can create a subgroup under **Public devices**.
- **All devices:** Lists all devices that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). For an administrator, **All devices** lists all managed devices that have been scanned into the core database. Devices configured with the standard LANDesk agent automatically appear in the **All devices** group when they are scanned into the core database by the inventory scanner.

For regular users, All Devices is a composite of their user's **My devices** and **Public devices** groups.

Administrators and users can run asset reports on the devices in this group.

You can also manually add computers to the network view by right-clicking the **All devices** group, selecting, clicking **Insert new computer**, filling in the device and network information, and clicking **OK**. These computers also appear in the User added computers subgroup under the Configuration group.

- **User devices:** Lists all of the devices in the core database, organized into user subgroups. User subgroups are named with user login IDs (i.e., computername\user account, or domain\user account). Each user group contains the devices that appear in that user's **My devices** group.

Note that ONLY administrators can see the **User devices** group and its subgroups. Other users do not see the **User devices** group at all.

Queries

The **Queries** group contains the following query subgroups.

- **My queries:** Lists queries either created by the currently logged-in user, or added to the user's **User queries** group by an administrator. A user can create, modify and delete query groups and queries under their **My queries** group. They can also copy queries to this group from the **Public queries** group.

Any query a user runs is limited to the range of devices defined by the user's scope. For example, if a user's scope is **All machines**, the query will search all devices in the core database, but if the user's scope is restricted to 20 machines, only those 20 machines will be searched by the query.

For more information on creating queries, see [Creating database queries](#).

- **Public queries:** Lists queries that an administrator, or a user with the Public Query Management (PQM) right, has added. Only users with the LANDesk Administrator right or the PQM right can add, modify, or delete query groups or queries in the **Public queries** group. However, all users can see the queries in this group, and can copy them to their own **My queries** group.
- **All queries:** Lists all queries that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). **All queries** is a composite of the user's **My queries** and **Public queries** groups.
- **User queries:** Lists all queries in the core database, organized into subgroups by user. User subgroups are named with their login IDs (i.e., computername\user account, or domain\user account). Each user group contains the queries that appear in that user's **My queries** group.

Note that **ONLY** administrators can see the **User queries** group and its subgroups. Other users do not see the **User queries** group at all.

Administrators can use this group to run a user's queries against that user's scope, as if they were that user. In this way, an administrator can preview exactly the results a user will see when they run a query.

Configuration

The **Configuration** group contains the following configuration groups.

- **PXE holding queue:** Lists PXE holding queues and the devices that are waiting in the PXE holding queue. For more information, see [Using the PXE holding queue](#).
- **Multicast domain representatives:** Lists configured multicast domain representatives that can be used for software distribution load balancing. For more information, see [Using Targeted Multicasting](#).
- **PXE representatives:** Lists devices configured as PXE representatives that can deploy OS images to devices in their subnet. For more information, see [Using PXE representatives](#).
- **Pending unmanaged client deployments:** Lists devices that have been discovered by the Unmanaged Device Discovery tool, and are waiting for an agent configuration task. For more information, see [Using Unmanaged Device Discovery](#).
- **User added computers:** Lists computers that have been added manually to the network view via the Insert new computer dialog (right-click the **All devices** group).

Creating groups

Groups help you organize devices and queries in the console's network view. You can create groups to organize network devices based on function, geographic location, department, device attribute or any other category that meets your needs. For example, you could create a marketing group for all devices in the marketing department or a group that includes all devices running a specific OS.

Rules for creating groups

- **My devices and My queries:** Administrators and all other users can create groups under **My devices** and **My queries**.
- **Public devices:** Only administrators can create groups under **Public devices**.
- **Public queries:** Only administrators or users with the Public Query Management (PQM) right can create groups under **Public queries**.
- **All devices and All queries:** There are no subgroups in **All devices** or **All queries**. Users, including administrators, cannot create groups under **All devices** or **All queries**.
- **User devices:** Only administrators can create groups under the user-specific subgroups in **User devices**.
- **User queries:** Only administrators, and users with the Public Query Management (PQM) right, can create groups under the user-specific subgroups in **User queries**.

To create a group

1. In the console's network view, right-click the parent group (such as **My devices**), and then click **New group**. Or, select the parent group, and then click **Edit | My Devices | New Group**.
2. Type in a name for the new group, and then press the **Enter** key.

You can right-click groups to perform various tasks, based on the type of group. For example, if you created a device subgroup, its shortcut menu lets you:

- Add devices
- Create a new subgroup
- Run an inventory report
- View as a report
- Cut
- Copy
- Paste
- Remove
- Rename











For more information on right-click features, see "Shortcut menus" below.

Device icons

Device icons display in the console's network view and show the current agent and health status of a device.

You can update the agent and health status for devices one at a time as you select them in the network view, or for all of the visible devices in the network view at the same time. You can also update a device's status by selecting it and clicking the Refresh toolbar button. For information on configuring how agent discovery is handled, see "Configuring agent discovery" later in this chapter.

The following table lists the possible device and status icons and what they mean:

Icon	Type and description
	Server: Represents a server device.
	Windows device: Represents a Windows device.
	Macintosh device: Represents a Macintosh device.
	Handheld device: Represents a handheld device.
The status icons below can display next to the device icons listed above, depending on the device's current configuration and status.	
	Not available: Indicates the device is not currently available to the console.
	Unknown: Indicates the status of the device is not currently known. This icon appears briefly while the device status is being updated.
	Standard LANDesk agent: Indicates the standard LANDesk agent is loaded on the device.
	Remote control: Indicates the remote control agent is loaded on the device.
	Warning: Indicates a health warning for the device. A health status icon can appear only if the LANDesk System Manager agent is loaded on the device.
	Critical: Indicates a critical health status for the device. A health status icon can appear only if the LANDesk System Manager agent is loaded on the device.

Icon display quality

These are high-color icons and require at least a 16-bit color-depth setting. If the icons in your console appear out of focus, change your color settings in the Windows Display Properties.

If your firewall blocks UDP packets

If you manage devices through a firewall that blocks UDP packets, you won't be able to use these device shortcut menu features: **Wake Up**, **Shut Down**, **Reboot**, and **Inventory Scan**.

Viewing managed devices in the All Devices group

Devices running LANDesk agents automatically appear in the **All devices** group when they are scanned into the core database by the inventory scanner. Typically, this scan takes place for the first time during a device's initial agent configuration. Once a device is scanned into the core database it is considered to be a managed device. In other words, it can now be managed by that core server. For more information on setting up devices, see [Device agent configuration](#).

Because the **All devices** group is populated automatically, via an inventory scan, you may never need to manually discover devices. However, to discover devices not already in the core database, you can scan the network for devices with the unmanaged device discovery tool. For more information, see [Using unmanaged device discovery](#).

When connected to a particular core server, the administrator can see every device managed by that core server. Regular users, on the other hand, are restricted and can only see the devices that reside within their assigned scope (a scope is based on either a database query or a directory location). For more information, see [Using role-based administration](#).

Shortcut menus

Shortcut (context) menus have been significantly expanded for all items in the console, including groups, devices, queries, scheduled tasks, scripts, reports, and so on. Shortcut menus provide quick access to an item's common tasks and critical information.

To view an item's shortcut menu, select and right-click the item.

Available options in the shortcut menu

Options that appear in a device's shortcut menu, as well as options that are disabled or dimmed, may differ depending upon the device platform and upon which LANDesk agents are installed on the device.

For example, when you right-click a managed device in the network view, its shortcut menu will typically display the following options:

- **Inventory:** Displays all of the device's inventory data scanned in the core database.
- **Inventory history:** Displays inventory data changes for the attributes you've selected for tracking. You can print the inventory history or export it to a .CSV file.
- **Remote control:** Opens a remote control session with the device.
- **Chat:** Opens a remote chat session with the device.
- **File transfer:** Opens the file transfer dialog where you can transfer files to and from the device.
- **Remote execute:** Lets you browse to and execute a batch file or application on the device.
- **Wake up:** Remotely wakes up a device whose BIOS supports Wake on LAN* technology.
- **Shut down:** Remotely shuts down the device.
- **Reboot:** Remotely reboots the device.
- **Inventory scan:** Runs an inventory scan on the device.
- **Scheduled tasks and policies:** Displays the device's current scheduled tasks and application management policies.
- **Add to new group:** Adds a copy of the device to a new user-defined group under the **My Devices** group. You're prompted to enter a name for the new group.
- **Add to existing group:** Lets you select the group where you want to add a copy of the device.
- **Group membership:** Displays all of the groups where the device is currently a member.
- **Run inventory report:** Opens the Reports dialog where you can select from a list of reports to run on the device. Double-click the report name to run it.
- **Security and patch information:** Opens the Security and patch information dialog that displays detailed vulnerability scan and remediation data for the device: including detected vulnerabilities and other security risks, installed patches, and repair history.
- **Security and patch scan now:** Opens a dialog that lets you select a scan and repair settings, and then click **OK** to perform an immediate security scan on the device.
- **Manage local users and groups:** Opens the Local users and groups dialog that lets you remotely manage a Windows device's local users and groups.
- **Cut:** Removes items from a user-defined group. You can't cut items from the "All" groups.
- **Copy:** Creates a copy of the item that you can add to a another group.
- **Paste:** Places the item you've cut or copied into a user-defined group.
- **Remove:** Removes the item from a user-defined group.
- **Delete:** Deletes the item from the "All" group AND from any other group it's a member of at the time.

- **Properties:** Displays the device's inventory summary, device information, agent status, and remote control settings.

This guide does not cover every possible item's (devices, queries, scripts, etc.) shortcut menu. We recommend that you right-click any item to see the options that are available.

Configuring the network view with column sets

Column sets allow you to customize the inventory data that displays in the right pane of the network view, for both device lists and query results lists. Each column in a column set represents a unique attribute (or component) from the scanned inventory. For example, the default column set that displays in the network view is comprised of the Device Name, Type, and OS Name attributes.

Use the Column Set Configuration tool (**Tools | Administration | Column Set Configuration**) to create as many column sets as you like. Then, to apply a column set, drag the desired column set to device groups and query objects in the network view tree.

Column sets window

Note: The Column Sets window replaces the Manage Column Configuration dialog found in previous versions.

The Column sets window organizes column sets into three categories:

- **My column sets:** Column sets created by the currently logged-in user.
- **Public column sets:** Column sets created by an administrator, or predefined column sets.
- **All column sets** (only visible to an administrator): Column sets created by all LANDesk users.

A user can copy a column set from the Public Column Sets group into their own My Column Sets group and then modify the column set properties.

You can create subgroups under the **My column sets** object to further organize your column sets.

Creating column sets

The **Column configuration** dialog is where you create column sets. Each column represents a single inventory attribute or component that has been scanned into the core database. Columns appear from left to right in the network view in the order that they appear in the Columns list.

To create a column set

1. Click **Tools | Administration | Column Set Configuration**.
2. Select the **My column sets** object (or the **Public column sets** object), and then click the **New** toolbar button.
3. In the **Column Configuration** dialog, enter a name for the new column set.
4. Select inventory attributes from the list and add them to the Columns list by clicking **Add to columns**. Remember to select attributes that will help you identify the devices in the device list or returned by the query.
5. (Optional) You can customize how and where the columns appear in the network view by directly editing a component's heading, alias, and sort order fields; or by removing or moving the selected component up or down in the list with the available buttons.

6. (Optional) You can specify more precise qualifying data for software components. Select the software component, click the **Qualify** button, and then select a primary key value from the list of available values. For more information, see Using the qualify option with software components below.
7. Click **OK** to save the column set.

Restoring the original default columns

To restore the default columns in the network view, simply create a custom column set that includes the Device Name, Type, and OS Name attributes, and then apply it to device groups and query objects. Or, you can use the predefined column set named Original in the My column sets group.

Applying column sets to device groups and queries

Once you've created a column set, you can drag it to a devices group or subgroup, or to a specific query object in a queries group or subgroup. The device list, or query results list, displays the inventory data specified by the selected column set in the right pane of the network view.

Note that for device lists, once a column set is applied to a group it persists even when you select different device groups. However, for query results lists, the column set must be reapplied when changing between various queries.

You can also right-click a column set to access its shortcut menu and perform common tasks, as well as view and edit its properties. The shortcut menu includes the following options:

- Add to new group
- Add to existing group
- Group Membership
- Set as default
- Cut
- Copy
- Remove
- Rename
- Properties

Using the qualify option with software components

When creating column sets that include software components, you can specify a qualifier for those software components by choosing a specific primary key value. A software qualifier lets you more precisely identify the data you want a query to search for and display in that software component's column. For example, you can configure the column set to display version information for only one specific application by selecting that application's executable file name as the qualifier.

To specify a software component's qualifier, select the software component in the Columns list, click the **Qualify** button, and then select a value from the list of available primary key values.

As with the Alias field, once you select a primary key value and add it to the software component's Qualifier field, you can manually edit it by clicking in the field.

About the Column Configuration dialog

Use this dialog to create a new column configuration.

- **Name:** Identifies the column configuration.
- **Inventory attributes:** Lists each of the inventory objects and attributes scanned into the core database. Expand or collapse objects by clicking the box to the left of the object.
- **Add to columns:** Moves the selected inventory attribute into the columns list. If you select an entire inventory component, all of the inventory attributes contained in that component are added to the columns list.
- **Columns:** Lists the inventory attributes in the order they will appear, from left to right, in the network view.
- **Qualify:** Lets you specify a precise data qualifier for the selected software component. For more information, see [Using the qualify option with software components](#).
- **Remove:** Removes the selected attribute from the list.
- **Move up:** Moves the selected attribute up one position.
- **Move down:** Moves the selected attribute down one position.
- **OK:** Saves the current column configuration and closes the dialog.
- **Cancel:** Closes the dialog without saving any of your changes.

Toolbar options

The console includes a toolbar that provides one-click access to common network view operations and some basic console configuration options. The toolbar buttons are dimmed when an item in the network view is selected that does not support that operation.

You can enable text descriptions for toolbar buttons by clicking **View | Show toolbar text**.

The console toolbar includes the following buttons:

- **Cut:** Removes items from the network view and stores them temporarily on the clipboard. If you accidentally cut an item, use the paste command to restore it. You must restore the deleted item before you perform any other command.
- **Copy:** Copies items from one location in the network view to another.
- **Paste:** Pastes items you've cut or copied.
- **Delete:** Permanently removes the item. You can't restore items you delete from the network view.
- **Refresh:** Updates the selected group or item in the network view. You can also collapse and expand a group to update its items. You can also click **View | Refresh** to update the currently selected item in the network view.
- **Refresh scope:** Updates the selected group or item in the network view, based on the currently logged-in user's scope (as defined in the Users tool).
- **Layout:** Lists your saved window layouts. Select a layout from the drop-down list to restore the console to that layout configuration. If you want to save your current layout, click the **Save the current layout** button.
- **Core:** Lists core servers you have connected to before (which makes them appear in this list). You can select a core server from the list, or type the name of a core server and press **Enter**. That core server is searched for on your network, and if found you're prompted to log in with a valid user name and password.

Using console tools

Tools are available through both the Tools menu and the Toolbox. To enable the **Toolbox**, click **View | Toolbox**.

A LANDesk Administrator sees all of the tools in both the Tools menu and the **Toolbox**. Other LANDesk users will see only the tools (features) that are allowed by their assigned rights. Tools dependent on rights that a user hasn't been granted don't appear at all in the Tools menu or in the **Toolbox** when that user is logged in to the console. For example, if a user doesn't have the Reports right, the Reports tool does not appear in either the **Tools** menu or the **Toolbox**.

When you click a tool name, the tool's window opens in the console. Tool windows can be resized, docked, floating, hidden, and closed. You can have multiple tool windows open at the same time, docked or floating. See the next section for more information on manipulating tool windows.

Dockable tool windows

Dockable windows is a console feature that lets you open as many of the tools as you want and move them in and out of the main console window.

Note: You can save console layouts you've designed and prefer for certain management tasks, and restore a saved layout whenever you need it. For more information, see "Saving window layouts" later in this chapter.

When you open multiple tool windows, they're tabbed in a single window. The active tool window displays on top, with a tab for each open tool running along the side or bottom. Click a tab to display that tool window. You can dock the tabbed tools window or drag it so that it is floating outside of the console window.

Docking a tool window means attaching it to one of the edges of the console. The window is said to be in a docked state if it is currently attached to an edge of the console. You can also undock the tools window and have it free-floating outside of the console. You can dock windows horizontally or vertically in the console.

To dock a tool window

1. Click the window's title bar and drag the window to an edge of the console
2. When the docking rectangle (dim outline of the window) appears indicating that the window will be docked, release the mouse button. The window attaches to that edge of the console.

Note that only tool windows (those windows accessible from the Tools menu or **Toolbox**) can exist as docked windows, floating windows, or tabbed windows. The network view window can be resized but can't be tabbed with other windows, floated outside the console, or closed.

If you minimize and then restore the main console window, then all docked and floating windows, including tabbed windows, are also minimized and restored with it.

Auto hide

The tool windows also support the auto hide feature. Auto hide is a push pin button in the upper right-hand corner of a window that lets you hold a window in place or hide it.

When the push pin is in (i.e., the pin points down), the window is pinned in place and auto hide is temporarily disabled. When the push pin is out (i.e., the pin points to the left) the window goes into auto hide mode when the cursor moves off of the window. Auto hide minimizes and docks the window along one of the edges of the console and displays a tab in its place.

The **Toolbox** also supports auto hide.

Saving window layouts

Layouts are saved console configurations, meaning the position and size of the network view, the **Toolbox**, and all open tool windows. You can use window layouts to save and restore customized console configurations that are especially useful for certain tasks or users.

To change the layout of the console, select a saved layout from the **Layout** drop-down list on the main toolbar.

To save your current layout

1. Configure the console interface the way you want it.
2. Click the **Disk** button next to the **Layout** drop-down list on the toolbar.
3. Enter a unique name for the layout.
4. Click **OK**.

About the Manage window layouts dialog

Use this dialog to manage saved window layouts and to reset the console window to the previous layout.

- **Saved layouts:** Lists all of your saved layouts.
- **Reset:** Returns the console window to the previous layout.
- **Delete:** Removes the selected layout.
- **Rename:** Lets you change the name of the selected layout.

Find bar

Find lets you search for items in a list containing a specific word or phrase. The **Find** bar is available in the network view and tool windows that contain flat lists of items. For example, the **Find** bar appears when you're viewing the:

- All Devices group
- All Queries group
- Pending Unmanaged Client Deployments group
- Unmanaged Device Discovery tool window
- All Asset Reports

To search for an item with the Find bar

1. Select the **All devices** group. The **Find** bar appears at the top of the list.
2. In the **Find** text box, type any text you want to search for.
3. From the **In column** drop-down list, select the column you want to search
4. Click the **Search** toolbar button.

The resulting list displays only those items that matched your search criteria.

Status bar

The status bar at the bottom of the console displays the following information (from left to right):

- Number of selected items in a listing
- Current job name and status
- Name of the currently logged-in user
- Days until the core server will attempt to contact the licensing server

The status bar is always visible.

Viewing device properties

In the console's network view, you can quickly view information about a device by right-clicking the device in the device list and selecting **Properties**.

More detailed information about the device is available in its inventory data. You can view inventory data in the network view columns (which are configurable), or by right-clicking the device and selecting **Inventory** to open the full **Inventory** window.

About the Device properties dialog

Use this dialog to view useful information about the selected device. The dialog includes three tabs: **Inventory**, **Device**, and **Agents**. Click each one to view related information.

Inventory tab

The **Inventory** tab contains a summary of the device's inventory data. For more information, see [Viewing a summary inventory for a detailed description](#).

Device tab

The **Device** tab contains basic information about a device, including its location and identity on the network. This tab also appears when you manually insert a device (from the **All devices** group's shortcut menu, click **Insert new computer**).

- **Device:**
 - **Name:** The name that appears in the core database and network view for the device.
If you are manually inserting a device, you can make this a user-friendly name. If you enter nothing here, the default device name will be the Windows computer name.
 - **Type:** The type of device, such as Windows 2000 Server or XP Workstation.
- **Network:**
 - **IP Name:** The Windows computer name for the device.
 - **IP address:** The IP address assigned to the device.
 - **Physical address:** The physical address of the device.

Agents tab

The **Agents** tab contains information about the current status of agents and remote control settings for the device.

- **Common Base Agent status:** Indicates whether the standard LANDesk agent (Common Base Agent) is loaded on the device.
- **LANDesk System Manager status:** Indicates whether the LANDesk System Manager agent is loaded on the device. This agent will only be loaded if you have LANDesk System Manager installed on your core server, and if you've deployed the System Manager agent to this device. For more information, see "Configuring devices."

- **Remote control agent status:** Indicates whether the remote control agent is loaded on the device. If this agent is not loaded on the device, remote control operations (such as file transfer and chat) are not available.
- **Security type:** Indicates the remote control security model used for the device. Options include: Local template, Windows NT security/local template, and Certificate-based/local template.
- **Allow:** Shows the remote control operations that are allowed on the device. These operations were enabled by the device agent configuration.
- **Settings:** Indicates how remote control operates when you attempt to interact with the device.

Configuring agent discovery

Agent discovery is the process used to find managed devices that have the standard LANDesk agent or remote control agent installed. These two agents provide the following capability:

- **LANDesk agent:** The standard LANDesk agent enables the PDS (ping discovery service). If the standard LANDesk agent is installed on a device, you can schedule software distributions and device setup configurations.
- **Remote control:** Lets you remotely access and control a device.

Agent discovery uses TCP/IP to verify agents running on the devices.

IP addresses are used as search criteria in order to perform standard LANDesk agent discovery with TCP/IP. LANDesk looks for the standard LANDesk agent and remote control agent on devices within a specific range of IP addresses. This range of addresses is implied by the IP network address you supply.

If you don't designate subnet network addresses when searching on TCP/IP, discovery is performed only on the network segment where the console initiating the discovery resides. For example, if you've installed four consoles, each residing on a different network segment, you would have to initiate four scans, one from each of the four consoles.

On network segments where consoles don't exist, you **MUST** use subnet network addresses to access the information on that network segment.

Note on firewalls: If you have one or more firewalls on your network, agent discovery can't be used to search outside firewalls, because firewalls generally limit the flow of packet traffic to designated ports.

To configure agent discovery options

1. Click **Configure | Agent discovery options**.
2. Select whether you want agent discovery to update agent status for only the selected item in the network view, or all visible items in the network view.
3. Specify the agent status refresh rate.
4. Configure how you want to discover the remote control agent, and prioritize the address resolution methods.
5. Specify how long agent discovery will attempt to discover the remote control agent on the device before timing out.
6. Click **OK**.

About the Agent discovery options dialog

Use this dialog to configure the following agent discovery options.

- **Gather agent status:**
 - **For selected items only:** Specifies that a device's agent status is updated as the device is selected in the network view. This option generates the least amount of network traffic and is the default.
 - **For visible items in network view:** Specifies that all visible devices in the network view will have their agent status updated according to the refresh rate. As new devices become visible, their agent status (and health) are updated.
- **Agent and health status refreshes every < > minutes:** Indicates whether agent status is automatically updated. You can specify the refresh rate.
- **Discovery methods:** Indicates how the agent is discovered.
 - **IP address:** Uses the core database to retrieve the computer's stored IP address.
 - **Domain Name Service (DNS):** Resolves the computer's ID name with the DNS server when verifying the remote control agent. If you do not have a DNS server, clear this option.
 - **Windows Internet Name Service (WINS):** Uses NetBIOS name resolution.
 - **IP addresses from database:** Uses the core database to retrieve the device's stored IP addresses and tries each one. Computers can have several IP addresses in the database if they have multiple network cards.
 - **Move up and Move down:** Moves the selected method up or down in the Discover agent using list. Methods are tried in the order they appear in the list.
- **Timeout:** Sets the timeout value before the remote control agent discovery fails for each checked address resolution method.

Monitoring devices for network connectivity

Device monitoring lets you regularly monitor the connectivity of any of your managed devices.

Ping settings are specific to the device you've selected. When a device stops responding to a ping (when it goes offline), AMS alerts are generated to notify you. You can also configure alerts to inform you when devices come back online.

About the Configure device monitoring dialog

Use this dialog to configure the following device monitoring options.

- **Monitor these devices:** Lists the devices that are currently being monitored.
- **Add:** Opens the **Add monitored devices** dialog where you can search for and select managed devices that you want to monitor.
- **Remove:** Deletes the selected device from the list.
- **Ping frequency:** Control when and how the ping operation occurs. These settings can be applied to each device individually.
 - **Ping every:** Schedules a periodic ping at the specified minute interval.
 - **Schedule daily at:** Schedules a daily ping at a specific time.
 - **Retries:** Specifies the number of ping retries.
 - **Timeout:** Specifies the number of seconds until ping retries will timeout.
- **Alert settings:** Opens the Configure Alerts dialog where you can set up AMS alerting to notify you when the device goes offline or online. Alert Settings includes its own online Help that you can access by clicking the Help button.
- **OK:** Saves your changes and closes the dialog.
- **Cancel:** Closed the dialog without saving your changes.

Configuring device monitoring alerts

If you want device monitoring to notify you when managed devices come online or go offline, you have to first configure the alert settings.

To configure device monitoring alert settings

1. In the **Configure device monitoring** dialog, click **Alert settings**.
2. In the **Configure alerts** dialog, expand the **Device monitor** tree.
3. Select the alert you want to configure and click **Configure**.
4. Select an alert action and click **Next**.
5. Select the device you want the alert action performed on. Don't select the device you're monitoring, because if it goes offline, it won't be able to process the alert action.
6. Finish the alert configuration wizard.

Note: When you configure alert settings, they apply to all of the devices you're monitoring.

Working with devices that support Intel® AMT

Management Suite supports devices using Intel® Active Management Technology (Intel® AMT), a hardware and firmware functionality that enables remote device management. AMT uses out-of-band (OOB) communication for access to devices regardless of the state of the operating system or power to the device.

When devices are configured with Intel AMT, a limited number of management features are available even if the device does not have a Management Suite agent installed. As long as devices are connected to the network and have standby power, they can be discovered and can be added to inventory to be managed with other devices on the network.

If a device has AMT but no Management Suite agent installed, it can be discovered with unmanaged device discovery, moved to the inventory database, then viewed in the **My devices** list. However, many Management Suite management options are unavailable. These options are only made available when the Management Suite agent is installed. Management features that are available for AMT-configured devices include:

- **Inventory summary:** a subset of the normal inventory data can be queried and viewed in real time for the device even if the device is powered off.
- **Event log:** a log with AMT-specific events, showing severity and description of the events, can be viewed in real time.
- **Remote boot manager:** power cycling and several boot options can be initiated from the remote management console, regardless of the state of the device's OS or power. The options available are based on the support for the options on the device. Some devices may not support all boot options.
- **Force vulscan and disable OS network:** if a device appears to have malicious software running, a vulnerability scan can be run at the next reboot; if necessary, the device's OS-level network access can be disabled to prevent unwanted packets from being spread on the network.

Intel AMT provisioning requirements

In order to discover and manage devices with Intel AMT capabilities, each device must have been provisioned in Small Business mode. Management Suite does not support Enterprise mode (with TLS enabled) at this time. If the manufacturer did not provision the device in Small Business mode, use the Intel AMT Configuration Screen to provision the device correctly (see the documentation provided by Intel for this Configuration Screen).

To view the inventory summary or add the device to the inventory database in order to manage the device, you must first configure the username/password for the AMT device (using the Configure Services utility), which allows Management Suite to authenticate to the AMT. This is done once for all AMT devices. This password configuration is added to the core database, which stores the information so Management Suite can authenticate to AMT devices.

If you have AMT devices with different credentials, you will need to change the credentials (using the Configure Services utility) for each device or group of devices before managing them.

To configure the Intel AMT password

1. Click **Configure | Services**.
2. Click the **Intel AMT password** tab.

3. Type the current user name and password. These must match the user name and password as configured in the Intel AMT Configuration Screen (which is accessed in the computer BIOS settings).
4. To change the user name and password, complete the **New Intel AMT password** section.
5. Click **OK**. This change will be made when the client configuration is run.

Managing Intel AMT devices

After an Intel AMT-configured device has been discovered and its user name/password configured, it can be managed in limited ways even if the device does not have a Management Suite agent installed.

The following table lists the management options available when a device has Intel AMT only compared with Intel AMT and a Management Suite agent.

	Intel AMT only	Intel AMT and agent	Agent only
Inventory	summary	X	X
Event log	X	X	X
Remote boot manager	X	X	
Disable OS network		X	
Enable OS network		X	
Force vulscan on reboot		X	
Inventory history		X	X
Remote control		X	X
Chat		X	X
File transfer		X	X
Remote execute		X	X
Wake up		X	X
Shut down		X	X
Reboot		X	X
Inventory scan		X	X
Scheduled tasks and policies	limited	X	X
Group options		X	X
Run inventory report		X	X

To view the Intel AMT inventory summary

1. Right-click the device in the **All devices** list and click **Intel AMT options | Intel AMT summary**.

The dialog shows the device's name, IP address, and the protocol and port number of the connection, as well as manufacturer information, Product information, GUID and serial number, AMT version and BIOS, processor, and memory summaries. At the bottom the username used to authenticate to the AMT device is shown.

Intel AMT event log

Management Suite provides a window to view the event log that Intel AMT devices generate. The AMT settings determine what events are captured in this log. You can view the date/time of the event, the source of the event (Entity column), a description, and the severity as determined by the AMT settings (Critical or Non-Critical). You can also export the log data in comma-separated value (CSV) format.

To view the Intel AMT event log

1. Right-click the device in the **All devices** list and click **Intel AMT options | Intel AMT event log**.
2. To export the log to a CSV format file, click the **Export** button on the toolbar and specify a location to save the file to.
3. To clear all data in the log, click the **Clear** button on the toolbar.
4. To update the log entries, click the **Refresh** button on the toolbar.

Intel AMT remote boot manager

The remote boot manager contains options to power on and off Intel AMT devices. These options can be used even when a device's operating system is not responding, as long as the device is connected to the network and has standby power. The Intel AMT device may or may not support all boot options.

You can simply turn on or off the device's power, or you can reboot and specify how the device is rebooted. The options are described in the table below.

Option	Description
Power off	Shuts down the power on the device
Power on	Turns on the power on the device
Reboot	Cycles the power off and on again on the device
Normal boot	Starts up the device using whatever boot sequence is set as the default on the device
Boot from local hard drive	Forces a boot from the device's hard drive regardless of the default boot mode on the device
Boot from CD/DVD	Forces a boot from the device's CD or DVD drive regardless of the default boot mode on the device
PXE boot	When restarted, the PXE-enabled device searches for a PXE server on the network; if found, a PXE boot session is initiated on the device
IDE-R boot	Reboots the device using the IDE redirection option selected (see below)
Enter BIOS setup	When the device is booted, it allows the user to enter the BIOS setup
Enable console redirection	When the device is booted, it starts in serial over LAN mode to display a console redirection window
IDE redirection: Boot from floppy	When the device is booted, it starts from the floppy disk drive or image that are specified (floppy image files must be in .img format; see note below)
IDE redirection: Boot	When the device is booted, it starts from the CD drive or

from CD/DVD image that are specified (CD image files must be in .iso format; see note below)

To use remote boot manager options

1. Right-click the device in the **All devices** list and click **Intel AMT options | Intel AMT remote boot manager**.
2. Select a power command. If you select **Reboot**, select a boot option.
3. Click **Send** to initiate the command.

Notes on using IDE redirection options

To use IDE redirection options, both a boot floppy or floppy image file and a boot CD/DVD or CD/DVD image file must be specified. Floppy image files must be in .img format, and CD image files must be in .iso format. Some BIOSes may require the CD image to be located on a hard drive.

Intel AMT normally remembers the last IDE-R settings, but Management Suite clears the settings after 45 seconds, so on subsequent boots it will not restart the IDE-R feature. The IDE-R session on an Intel AMT device lasts 6 hours or until the Management Suite console is turned off. Any IDE-R operation still in progress after 6 hours will be terminated.

Forcing a vulnerability scan and disabling network access on Intel AMT devices

When an Intel AMT-configured device has the Management Suite agent installed, the agent includes functionality that can help resolve problems with malicious software or other issues that prevent you from accessing the device.

The amtmon.exe service is installed with the Management Suite agent. When this service is running on a device, you can force a vulnerability scan at the next reboot to attempt to identify any malicious software on the device. If communication with the device fails, you can disable the device's network connection even if the OS is not functional, such as when malicious software has disabled the OS by consuming all CPU cycles. By disabling the network connection you can prevent the device from sending unwanted packets through the network.

When the Management Suite agent is installed on an Intel AMT device, the following options are available on the shortcut menu in the **My devices** list:

- **Force vulscan on reboot:** runs the Management Suite vulnerability scanner the next time the device reboots
- **Disable OS network:** disables the OS network stack to stop network access
- **Enable OS network:** enables OS network access if it has been disabled

When a device is not responding or may have malicious software running on it, the recommended use case is to first run a vulnerability scan on the next reboot to attempt to identify the problem. If the problem continues and the machine is infecting/attacking the network, or if you can't access the device, you have the option to disable the OS NIC.

To force a vulnerability scan after a reboot

1. Right-click the device in the **All devices** list and select **Force vulscan on reboot**. A message appears on the device stating that a scan will be run the next time it reboots.

2. To shut down or reboot the device, use the Intel AMT remote boot manager features.

To disable or enable the network connection on an unresponsive device

1. To disable the device's network card to stop communication with other devices on the network, right-click the device in the **All devices** list and select **Disable OS network**. When the network connection is disabled, a message appears on the device stating that the network card has been disabled.
2. When the device is safe to connect to the network again, right-click the device in the **All devices** list and select **Enable OS network**. When the connection is restored, a message appears on the device stating that the network card is enabled again.

Using role-based administration

Role-based administration enhances LANDesk network security by enabling you to control user access to managed devices, console views, and specific features and tools. This chapter describes how role-based administration works and how you can implement it to effectively administer your LANDesk-managed network.

Read this chapter to learn about:

- Role-based administration overview
- Managing LANDesk users
- Managing groups
- Understanding rights
- Creating scopes
- Assigning rights and scopes to users

Role-based administration overview

Role-based administration lets you control what devices a user can manage and which tools they can access and use with those devices. LANDesk Administrators (users with the LANDesk Administrator right) can access the role-based administration tools (click **Tools | Administration | Users**). Role-based administration lets you assign special rights to users on your system. Groups and organizational units (OUs) from a directory service can also be assigned rights, which are propagated to users belonging to the group or OU.

- **Rights:** Determine the tools and features a user can see and use (see Understanding rights later in this chapter).
- **Scopes:** Determine the range of devices a user can see and manage (see Creating scopes later in this chapter).

Note: Users who don't have the Administrator right won't see the Users tool.

You can create roles based on user responsibilities, the management tasks you want them to be able to perform, and the devices you want them to be able to see, access, and manage. Access to devices can be restricted to a geographic location like a country, region, state, city or even a single office or department. Or, access can be restricted to a particular device platform, processor type, or some other device hardware or software attribute. With role-based administration, it's completely up to you how many different roles you want to create, which users can act in those roles, and how large or small their device access scope should be. For example, you can have one or more users whose role is software distribution manager, another user who is responsible for remote control operations, a user who runs reports, and so on.

Example administrative roles

The table below lists some of the possible Management Suite administrative roles you might want to implement, the common tasks that user would perform, and the rights that user would need in order to function effectively in that role.

Role	Tasks	Required rights
Administrator	Configure core servers, install additional consoles, perform database rollup, manage users, configure alerts, integrate LANDesk System Manager, and so on. (Of course, administrators with full rights can perform any management tasks.)	LANDesk administrator (all rights implied)
Device inventory manager	Discover devices, configure devices, run the inventory scanner, create and distribute custom data forms, enable inventory history tracking, and so on.	Unmanaged device discovery, software distribution, software distribution configuration, and public query management
Helpdesk	Remotely control devices, chat, transfer files, execute software, shutdown, reboot, view agent and health status, and so on.	Remote control
Application	Distribute software packages, use	Software distribution

manager	Targeted Multicast and peer download, and so on.	and software distribution configuration
Migration manager	Create images, deploy OS images, migrate user profiles, create and distribute user-initiated profile migration packages, deploy PXE representatives, assign PXE holding queues, configure the PXE boot menu, create boot floppy disks, and so on.	OS deployment
Reporting manager	Run predefined reports, create custom reports, print reports, publish reports, import and export reports, test user reports, and so on.	Reports (required for all reports)
Software license monitoring manager	Configure applications to monitor, add licenses, upgrade and downgrade licenses, verify reports, and so on.	Software license monitoring

Note: Some of the example administrative roles would require the Basic Web console right in order to use the features in the Web console.

These are just example administrative roles. Role-based administration is flexible enough to let you create as many custom roles as you need. You can assign the same few rights to different users but restrict their access to a limited set of devices with a narrow scope. Even an administrator can be restricted by scope, essentially making them an administrator over a specific geographic region or type of managed device. How you take advantage of role-based administration depends on your network and staffing resources, as well as your particular needs.

To implement and enforce role-based administration, simply designate current NT users, or create and add new NT users as LANDesk users, and then assign the necessary rights (to features) and scopes (to managed devices).

Managing LANDesk users

LANDesk users can log in to the console and perform specific tasks for specific devices on the network. Users appear in the **All Users** group (click **Tools | Administration | Users | All users**) after they have been created and added to the Windows NT **LANDesk Management Suite** group on the core server (see Adding LANDesk users). The **All Users** group shows all of the users currently residing in the LANDesk Management Suite group on the core server.

The user that is logged in to the server during LANDesk installation is automatically placed into the Windows NT **LANDesk Management Suite group**, added as a LANDesk user, and assigned rights as an administrator. This individual is responsible for adding additional users to the console and assigning rights and scopes. Once other administrators have been created, they can perform the same administrative tasks

All users added to the console after LANDesk has been installed assume the same rights and scope as the **Default Template User**. This user serves as a template of user properties (rights and scopes) that is used to configure new users. When users are added to the LANDesk Management Suite group in the Windows NT environment, the users automatically inherit the same rights and scopes currently defined in the Default Template User properties. You can change the property settings for the Default Template User by right-clicking it and then clicking **Properties**. Being able to configure the rights and scopes that users receive upon being added to the console greatly facilitates user management. For example, if you want to add a large number of users at once, but do not want them to have access to all of the tools or devices, change the settings for the Default Template User first, then add the users to the LANDesk Management Suite group.

Note: The Default Template User cannot be removed.

When you add a user to the console, their user name, scopes, and rights are displayed. Additionally, new user subgroups, named by the user's unique login ID, are created in the **User devices**, **User queries**, **User reports**, and **User scripts** groups (note that besides the actual user, ONLY an administrator can view user groups). To refresh the **All users** group to display any newly added users, right-click **All users** and click **Refresh**.

Creating LANDesk users

LANDesk users can be created from the console or from the native local accounts management system on the core server.

To create a LANDesk user from the console

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click your core server and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Users** and then click **Add**.
4. In the **New User** dialog, enter a user name, a full name, and a description.
5. Enter a password, confirm the password, and specify the password settings.
6. Click **Save**.

Note: Remember to add the user to the LANDesk Management Suite group to have them appear in the All Users group in the console.

To create a LANDesk user from the Windows NT Computer Management dialog

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click **Users**, and then click **New User**.
3. In the **New User** dialog, enter a name and password.
4. Specify password settings.
5. Click **Create**. The New User dialog remains open so that you can create additional users.
6. Click **Close** to exit the dialog.

Note: Remember to add the user to the LANDesk Management Suite group to have them appear in the All Users group in the console.

Adding LANDesk users

LANDesk users need to be added to the LANDesk Management Suite group in order to be recognized as LANDesk users and appear in the console. Other domain groups can also be added to the LANDesk Management Suite group. If you add a domain group to the LANDesk Management Suite group, all users in the domain group are enumerated and added as console users. LANDesk only allows a single enumeration, so any additional domain groups under the top-tier domain group are ignored.

To add users to the LANDesk Management Suite group from the console

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click your core server and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the **LANDesk Management Suite** group, and then click **Edit**.
5. In the **Edit group - LANDesk Management Suite** dialog, click **Add**.
6. In the **Select users** dialog, select the desired users and then click **Add>>**.
7. Click **OK**.
8. In the **Edit group - LANDesk Management Suite** dialog, click **OK**.

To add users to the LANDesk Management Suite group from the Windows NT Computer Management dialog

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Groups | Groups** utility.
2. Right-click the **LANDesk Management Suite** group, and then click **Add to group**.
3. In the **LANDesk Management Suite Properties** dialog, click **Add**.
4. In the **Select the users and groups** dialog, select the desired users (and groups) from the list and click **Add**.
5. Click **OK**.
6. In the **LANDesk Management Suite Properties** dialog, click **OK**.

Note: You can also add a user to the LANDesk Management Suite group by right-clicking the user account in the Users list, clicking **Properties | Member Of**, and then clicking **Add** to select the group and add the user.

You can now assign your LANDesk users rights and scopes.

Removing LANDesk users

If you remove a user from the LANDesk Management Suite group from the console or the Windows NT users environment, the user still appears in the **All users** group, but has a red X through it, indicating it is no longer included as a member of that group, and cannot authenticate to any LANDesk console. The user's account still exists in the database and can be added back to the LANDesk Management Suite group at any time. Also, the user's subgroups under **User devices**, **User queries**, **User reports**, and **User scripts** are preserved so that you can restore the user without losing their data, and so that you can copy data to other users. You can also permanently delete a user from the database.

WARNING: When you delete a user from the database, all of the data owned by that user is permanently deleted, including scripts, tasks, queries, and so on.

To remove a user using the console

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click your core server and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to remove and then click **Delete**.
5. Click **Yes** to verify the procedure.

To remove a user using the Windows NT Computer Management dialog

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click the user you want to remove and then click **Delete**.
3. Click **Yes** to verify the procedure.

To permanently delete a user from the database

1. Make sure the user has been removed from the **LANDesk Management Suite** Windows NT group using the console or the Windows NT computer management dialog.
2. In the console, click **Tools | Administration | Users**.
3. Right-click the user (with a red X) and then click **Delete**. Remember, this action will result in permanent loss of the user data.
4. Click **Yes** to verify the procedure.

Managing groups

LANDesk interfaces with Microsoft Active Directory Services* (ADS) in order to assign rights to groups and organizational units (OUs). Any users, groups or OUs added to the group or OU will inherit the same rights.

You can categorize users by placing them into groups and OUs that have specific rights assigned to them. You only need to assign the group or OU the specific rights and then add the desired users, as opposed to configuring the rights for every single user, one user at a time. This simplifies user management and accelerates the appropriation of rights, as well as reduces the potential of misappropriating rights to users.

Using active directories

LANDesk enables you to utilize active directories to add groups and organizational units (OUs) to the console and assign them rights. You can authenticate to the server from the console. Once you have logged in to the active directory server, you can add groups and OUs to the console and assign rights to them. LANDesk supports using one LDAP directory at a time.

Managing active directories should be performed by an expert user with extensive experience working with directory services, specifically ADS. Tasks include adding and removing users and groups, maintaining the framework (forest, trees, domains, groups, OUs, etc.), and understanding LANDesk's interaction with the directory service. You should be aware of the following issues when managing active directories for use with LANDesk:

- Active directory is fully integrated with DNS and TCP/IP (DNS is required, and to be fully functional, the DNS server must support SRV resource records or service records).
- Using active directory to add a user to a group being used in the console will not enable the user to log in to the console even though the user has LANDesk rights assigned. In order to log in to the console, a user must belong to the **LANDesk Management Suite** Windows NT group on the core server.

For more information about LDAP, including LDAP queries, see [More about LDAP](#).

Logging in to the active directory

You need to log in to the active directory before you can add groups and organizational units to the console.

To login to the active directory

1. Click **Tools | Administration | Users**.
2. Click the **Login to Active Directory** button.
3. In the **Login to Active Directory** dialog, insert the path to the LDAP directory and provide the user name and password to authenticate to the server.
4. Click **OK**.

Adding groups and organizational units to the console

You need to add LDAP groups and organizational units (OUs) to the console before you can assign rights to them.

To add groups and OUs

1. Click **Tools | Administration | Users**.
2. Click **Active directory**.
3. Click the **Add a new group or OU** button.
4. In the **Available Active Directory groups and OUs** dialog, select the desired groups and OUs and click **OK**.

Assigning rights to a group or organizational unit



You can assign rights to groups and organizational units (OUs). Any user, group, or OU placed into the group or OU will inherit the rights you assign. This enables you to assign the same rights to multiple nodes at one time, rather than having to configure rights individually.

To assign rights to a group or OU

1. Click **Tools | Administration | Users**.
2. Click **Active Directories**.
3. Right-click the desired group or OU and click **Properties**.
4. Under the Rights tab, select the appropriate rights and click **OK**.

Understanding rights

Rights provide access to specific LANDesk tools and features. Users must have the necessary right (or rights) to perform corresponding tasks. For example, in order to remote control devices in their scope, a user must have the remote control right. A user, group, or organizational unit (OU) can be assigned rights, and they can also inherit rights by being added to a group or OU. From the Users tool, you can see what rights are assigned or inherited:

-  This icon denotes an assigned right.
-  This icon denotes an inherited right.

Role-based administration includes the following rights:

- LANDesk Administrator
- Asset configuration
- Asset data entry
- Connection control manager
- Basic Web console
- OS deployment
- Public query management
- Remote control
- Reports
- Security and patch manager
- Security and patch compliance
- Software distribution
- Software distribution configuration
- Software license monitoring
- Unmanaged device discovery

See the descriptions below to learn more about each right and how rights can be used to create administrative roles.

Scope controls access to devices

Keep in mind that when using the features allowed by these rights, users will always be limited by their scope (the devices they can see and manipulate).

LANDesk Administrator

The LANDesk administrator (Admin) right provides full access to all of the application tools (however, use of these tools is still limited to the devices included in the administrator's scope).

This is the default right for a newly-added user, unless you've modified the settings for the Default Template User.

The LANDesk administrator right provides users the ability to:

- See and access the **Users** tool in the **Tools** menu and **Toolbox**
- See and manage **User device** groups in the **Network view**
- See and manage **User query** groups in the **Network view**
- See and manage **User scripts** groups in the **Manage scripts** window
- See and manage **User reports** groups in the **Reports** window
- See and configure product licensing in the **Configure** menu

- **Important:** Perform ALL of the Management Suite tasks allowed by the other rights

Basic rules about rights and tools

The LANDesk administrator right is exclusively associated with the **Users** tool. In other words, if a user doesn't have the LANDesk administrator right, the **Users** tool won't appear in the console.

All users, regardless of their assigned rights, can see and use the following universal features: inventory options, alert history, queries, and alert settings.

All of the other tools in the Management Suite console are associated with a corresponding right (as described below).

Asset configuration

The asset configuration right is specific to the Asset Manager add-on product. When an add-on product isn't installed, its corresponding rights still appear in LDMS in the list (checked) in LDMS but are dimmed. The respective add-on product's tools and features aren't available, of course. After an add-on product is installed, its respective rights are activated in this list, and can be checked to allow access to the add-on's features or cleared to deny access. For more information, see Using the Asset Manager add-on.

The Asset Configuration is an administration-level right that provides users the ability to:

- See and access all the Asset Management links in the Web console: Assets, Contracts, Invoices, Projects, Global Lists, Detail Templates, and Reports.
- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

Asset data entry

The asset data entry right is specific to the Asset Manager add-on product. When an add-on product isn't installed, its corresponding rights still appear in LDMS in the list (checked) but are dimmed. The respective add-on product's tools and features aren't available, of course. After an add-on product is installed, its respective rights are activated in this list, and can be checked to allow access to the add-on's features or cleared to deny access. For more information, see Using the Asset Manager add-on.

The asset data entry right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global Lists links in the Web console.
- Browse types and details (can't add, edit, or delete them)
- Add items to the database by completing in data entry forms
- Edit items that have been added to the database

Connection control manager

The connection control manager right provides users the ability to:

- See and access the connection control configuration tool in the **Tools** menu and **Toolbox**
- Control the access to external devices to control and configure them

Basic Web console

The basic Web console right applies to the Web console. The right provides users the ability to:

- See and use **My devices** (the right doesn't allow for the updating of public groups or deleting devices under the Actions tab)
- Change preferences (but not custom attributes)
- Use the dashboard
- Use software distribution on the Web console

OS deployment

The OS deployment right provides users the ability to:

- See and access the **Manage Scripts** tool in the **Tools** menu and **Toolbox**
- Create and run OS deployment and profile migration scripts
- Schedule OS deployment and profile migration tasks
- Configure PXE representatives with the Deploy PXE Representative script
- Designate PXE holding queues
- Configure the PXE boot menu
- Create and deploy customer data forms

Public query management

The public query management right provides users the ability to:

- Create, modify, copy, delete, and move queries in the **Public queries** group in the **Network view**. (Without this right, the devices in the **Public query** group are view-only.)

Remote control

The remote control right provides users the ability to:

- Use the remote control options on a device's shortcut menu (otherwise, they are dimmed)
- Remote control devices that have the remote control agent loaded
- Wake up, shut down, and reboot devices
- Chat with devices
- Execute device programs remotely
- Transfer files to and from devices

Reports

The reports right provides users the ability to:

- See and access the **Reports** tool in the **Tools** menu and **Toolbox**
- Run predefined reports
- View reports that have been run
- Create and run custom asset reports
- Publish reports in order to make them available to users with access credentials

Security and Patch Manager

The Security and Patch Manager right provides users the ability to:

- See and access the **Security and Patch Manager** tool in the **Tools** menu and **Toolbox**
- Configure managed devices for security assessment and remediation scanning
- Configure devices for real-time spyware and blocked application scanning
- Configure devices for high frequency scanning for critical security risks
- Download security updates (definitions and detection rules) and associated patches for the security types that you have a Security Suite content subscription for
- Create scheduled tasks that automatically download definitions and/or patch updates
- Create custom vulnerability definitions and custom detection rules
- Import, export, and delete custom definitions
- View downloaded security and patch content by type (including: all types, blocked applications, custom definitions, LANDesk updates, security threats, spyware, vulnerabilities, driver updates, and software updates)
- Customize selected security threats with custom variables
- Configure and run security scans on managed devices as a scheduled task or as a policy
- Divide a scheduled task scan into a staging phase and a deployment phase
- Create and configure scan and repair settings that determine the scan options, such as: content type to be scanned for, scanner information and progress display, device reboot behavior, and the amount of end user interaction. Then, apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks
- View detailed scan results (detected security data) by: detected group, specific definition, individual device, or a group of selected devices
- Perform remediation as a scheduled task or as a policy
- Use Auto Fix to automatically remediate the following security types if they are detected: vulnerabilities, spyware, LANDesk software updates, and custom definitions (must be a LANDesk Administrator)
- Track and verify the status of patch deployment and installation (repair history) on scanned devices
- Purge unused security type definitions (must be a LANDesk Administrator)
- Uninstall patches from scanned devices
- Remove patches from the core database
- Configure vulnerability alerts
- Generate a variety of security specific reports (also requires the Reports right)

Security and Patch Compliance

The Security and Patch Manager right provides users the ability to:

- Add and remove security definitions from the **Compliance** group
- Change the status of definitions contained in the Compliance group

This right also imposes user limitations:

- Cannot edit custom definitions or security threat's custom variables
- Cannot configure trusted access services, such as adding posture servers or remediation servers, or configure and publish compliance rules (must be a LANDesk Administrator)

Software distribution

The software distribution right is a subset of the software distribution configuration right (below), and provides users the ability to:

- See and access the **Manage Scripts** tool in the **Tools** menu and **Toolbox** (can only select items)
- See and access the **Scheduled Tasks** tool in the **Tools** menu and **Toolbox** (can only select items)
- See and access the **Delivery Methods** and **Distribution Packages** tools in the **Tools** menu and **Toolbox** (can only select items)
- Run software distribution scripts
- Run device agent configurations (can't create, edit, or delete)
- Schedule other script-based tasks (with the exception of OS deployment and profile migration scripts)
- Deploy custom data forms (can't create, edit, or delete)
- View LDAP directories

Note: Users require the basic Web console right to use software distribution on the Web console.

Software distribution configuration

The software distribution configuration right is the comprehensive distribution right, and provides users the ability to:

- Perform ALL of the tasks allowed by the software distribution right listed above (can see and access the same tools; select items; as well as create, edit, and delete items)
- Create, modify, and delete delivery methods and distribution packages
- Create and run software distribution scripts
- Create and run device agent configurations
- Schedule other script-based tasks (with the exception of OS deployment and profile migration scripts)
- Create and deploy custom data forms
- Create and distribute software packages through application policies

Software license monitoring

The software license monitoring right provides users the ability to:

- See and access the **Software license monitoring** tool in the **Tools** menu and **Toolbox**

- Configure applications to monitor, add licenses, upgrade and downgrade licenses, and verify reports

Unmanaged device discovery

The unmanaged device discovery right provides users the ability to:

- See and access the **Unmanaged device discovery** tool in the **Tools** menu and **Toolbox**
- Create scanner configurations and run different types of discovery scans (LANDesk agent, NT Domain, etc.)
- Create and run the different types of discovery scan tasks

Creating scopes

A scope defines the devices that can be viewed and managed by a Management Suite user.

A scope can be as large or small as you want, encompassing all of the managed devices scanned into a core database, or possibly just a single device. This flexibility, combined with modularized tool access, is what makes role-based administration such a versatile management feature.

Default scopes

Management Suite's role-based administration includes one default scope. This predefined scope can be useful when configuring the user properties of the Default Template User.

- **Default all machines scope:** Includes all managed devices in the database.

You can't edit or remove the default scope.

Custom scopes

There are three types of custom scopes you can create and assign to users:

- **LDMS query:** Controls access to only those devices that match a custom query search. You can select an existing query or create new queries from the Scope properties dialog to define a scope. Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group. For more information on creating queries, see *Creating database queries*.
- **LDAP:** Controls access to only those devices gathered by the inventory scanner that are located in an LDAP-compliant directory structure. Select directory locations from the **Select visible devices** dialog to define a scope. This directory-based scope type also supports custom directory locations (if you've entered custom directory paths as part of an agent configuration). Available custom directory paths appear in the **Select visible devices** dialog. Use custom directories to define a scope if you don't have an LDAP-compliant structure, or if you want to be able to restrict access to devices by a specific organizational detail such as geographic location or department.
- **Device group:** Controls access to only those devices that belong to a specific device group in the network view.

A Management Suite user can be assigned one or more scopes at a time. Additionally, a scope can be associated with multiple users.

How multiple scopes work

You can assign more than one scope to any of your Management Suite users. When multiple scopes are assigned to a user, the cumulative effective scope (the complete range of devices that can be accessed and managed as a result of the combination of assigned scopes) is a simple composite.

You can customize a user's effective scope by adding and removing scopes at any time. All three types of scopes can be used together.

Creating scopes

To create a scope

1. Click **Tools | Administration | Users**.
2. Right-click **Scopes** and select **New Scope**.
3. In the **Scope Properties** dialog, enter a name for the new scope.
4. Specify the type of scope you want to create (LDMS query, LDAP or custom directory, or device group) by clicking the desired scope type from the drop-down list, and then clicking **New**.
5. If you're creating an LDMS query-based scope, define the query in the **New scope query** dialog, and then click **OK**.
6. If you're creating an directory-based scope, select locations (LDAP directory and/or custom directory) from the **Select visible devices** list, and then click **OK**.

Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. You can multi-select locations by using Ctrl-click. All nodes under a selected parent node will be included in the scope.

LDAP directory locations are determined by a device's directory service location. For more information, see Using active directories. Custom directory locations are determined by a device's computer location attribute in the inventory database. This attribute is defined during device agent configuration.

7. If you're creating a device group-based scope, select a group from the available device group list, and then click **OK**.
8. Click **OK** again to save the scope and close the dialog.

About the Scope Properties dialog

Use this dialog to create or edit a scope. You can access this dialog by selecting a scope and clicking the **Edit scope** toolbar button or by right-clicking the scope and then clicking **Properties**.

- **Scope name:** Identifies the scope.
- **Select a scope type:**
 - **LDMS query:** Creates a scope whose device range is determined by a custom query. Clicking **New** with this scope type selected opens the **New query** dialog where you can define and save a query. This is the same query dialog you use when creating a database query from the network view. (Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group.)
 - **LDAP:** Creates a scope whose device range is determined by the device location (LDAP directory and/or custom directory). Clicking **New** with this scope type selected opens the **Select visible devices** dialog where you can select locations. Click on the plus (+) and minus (-) signs to expand and collapse nodes in the directory tree. You can multi-select locations by using Ctrl-click. All nodes under a selected parent node will be included in the scope.
 - **Device group:** Creates a scope whose device range is determined by an existing group of devices contained under the Devices object in the network view. Clicking **New** with this scope type selected opens the **Query filter** dialog where you can select a device group.
- **Current scope definition:** Displays the query statements for a query-based scope, the location paths for a directory-based scope, or the group name for a device group-based scope.

- **Edit:** Opens the scope's appropriate dialog where you can change query parameters and statements.
- **OK:** Saves the scope and closes the dialog.
- **Cancel:** Closes the dialog without saving any of your changes.

Assigning rights and scope to users

Once you've added LANDesk users, learned about rights and how they control access to features and tools, and created device scopes to allow or restrict access to managed devices, the next step in establishing role-based administration is to assign the appropriate rights and scopes to each user.

A user's role is completely configurable. They can have any combination of rights. Additionally, they can be assigned one or more scopes (see *How multiple scopes work* for more information).

You can modify a user's rights and scopes at any time.

If you modify a user's rights or scopes, those changes will only take effect the next time that user logs into the core server.

To assign rights and scope to a user

1. Click **Tools | Administration | Users**.
2. Select the **All users** group to view all of the users that are currently a member of the LANDesk Management Suite group in the core server's Windows NT environment.

The right-side pane displays a list of users, including their user name, current scope, and assigned rights (an x character indicates the right is enabled or active).

You can refresh this list by right-clicking **All users** and clicking **Refresh**.

3. Right-click a user, and then click **Properties**.
4. In the **User properties** dialog, click the **Rights** tab, and then check or clear rights as desired (see *Understanding rights* earlier in this chapter).
5. Click the **Scopes** tab, and then define a composite scope for the selected user by adding and removing scopes. For more information, see *How multiple scopes work*.
6. Click **OK**.

The new rights and scope display next to the user's name in the list and will take effect the next time the user connects to the core server.

Note: If the user has more than one assigned scope, the **Scope** column says "Multiple".

Configuring services

Many of the most integral and fundamental functions provided by LANDesk Management Suite (such as the inventory server and the scheduler service) can and should be configured in order to optimize performance in your particular network environment. This can be done by using the **Configure services** dialog in the console (**Configure | Services**).

Configuring services is restricted to only LANDesk Administrators

Only a user with the LANDesk Administrator right can modify service settings. Also, the **Configure services** option is available only from the main console, not from any additional consoles you may have set up.

Read this chapter to learn about:

- Selecting a core server and database
- Configuring the Inventory service
- Resolving duplicate device records in the database
- Configuring the Scheduler service
- Configuring the Custom Jobs service
- Configuring the Multicast service
- Configuring the OS Deployment service
- Configuring the AMT service

Note: For information about Intel AMT devices, see Working with devices that support Intel AMT.

Selecting a core server and database with General settings

Before configuring a service, use the **General** tab to specify the core server and database you want to configure the service for.

Note: Any service configuration changes you make for a core server and database will not take effect until you restart the service on that core server.

About the Configure Management Suite services dialog: General tab

Use this dialog to select the core server and database you want to configure a specific service for. Then, select the desired service tab and specify the settings for that service.

- **Server name:** Displays the name of the core server you're currently connected to.
- **Server:** Lets you enter the name of a different core server and its database directory.
- **Database:** Lets you enter the name of the core database.
- **Username:** Identifies a user with authentication credentials to the core database (specified during Setup).
- **Password:** Identifies the user's password required to access the core database (specified during Setup).
- **This is an Oracle database:** Indicates that the core database specified above is an Oracle database.
- **Refresh settings:** Restores the settings that were present when you opened the Service Configuration dialog.

When specifying usernames and passwords to a database, the username and the password may not contain an apostrophe ('), a semicolon (;) or an equals sign (=).

Configuring the Inventory service

Use the **Inventory** tab to configure the Inventory service for the core server and database you selected using the General tab.

About the Configure Management Suite services dialog: Inventory tab

Use this tab to specify the following inventory options:

- **Server name:** Displays the name of the core server you're currently connected to.
- **Log statistics:** Keeps a log of core database actions and statistics.
- **Encrypted data transport:** Enables the inventory scanner to send device inventory data from the scanned device back to the core server as encrypted data through SSL.
- **Scan server at:** Specifies the time to scan the core server.
- **Perform maintenance at:** Specifies the time to perform standard core database maintenance.
- **Days to keep inventory scans:** Sets the number of days before the inventory scan record is deleted.
- **Primary owner logins:** Sets the number of times the inventory scanner tracks logins to determine the primary owner of a device. The primary owner is the user who has logged in the most times within this specified number of logins. The default value is 5 and the minimum and maximum values are 1 and 16, respectively. If all of the logins are unique, the last user to log in is considered the primary owner. A device can have only one primary owner associated with it at a time. Primary user login data includes the user's fully qualified name in either ADS, NDS, domain name, or local name format (in that order), as well as the date of the last login.
- **Software:** Displays the **Software scan settings** dialog. Configure when the software scans run and how long to save the inventory history.
- **Manage duplicates: Devices:** Opens the **Duplicate devices** dialog, where you can configure how duplicate devices are handled.
- **Manage duplicates: Device IDs:** Opens the **Duplicate device ID** dialog where you can select attributes that uniquely identify devices. You can use this option to avoid having duplicate device IDs scanned into the core database (see Resolving duplicate device records in the database).
- **Inventory service status:** Indicates whether the service is started or stopped on the core server.
- **Start:** Starts the service on the core server.
- **Stop:** Stops the service on the core server.

About the Software scan settings dialog

Use this dialog to configure the frequency of software scans. A device's hardware is scanned each time the inventory scanner is run on the device, but the device's software is scanned only at the interval you specify here.

- **Every login:** Scans all of the software installed on the device every time the user logs on.
- **Once every (days):** Scans the device's software only on the specified daily interval, as an automatic scan.
- **Save history (days):** Specifies how long the device's inventory history is saved.

Resolving duplicate device records in the database

In some environments OS imaging is used regularly and frequently to set up devices. Because of this, the possibility of duplicate device IDs among devices is increased. You can avoid this problem by specifying other device attributes that, combined with the device ID, create a unique identifier for your devices. Examples of these other attributes include device name, domain name, BIOS, bus, coprocessor, and so on.

The duplicate ID feature lets you select device attributes that can be used to uniquely identify the device. You specify what these attributes are and how many of them must be missed before the device is designated as a duplicate of another device. If the inventory scanner detects a duplicate device, it writes an event in the applications event log to indicate the device ID of the duplicate device.

In addition to duplicate device IDs, you may also have duplicate device names or MAC addresses that have accumulated in the database. If you're experiencing persistent duplicate device problems (and as a precaution against duplicate device records being scanned into your database by the inventory scanner in the future), you can also specify that any duplicate device names currently residing in the database are removed. This supplementary duplicate device handling feature is included as part of the procedure below.

To set up duplicate device handling

1. Click **Configure | Services | Inventory | Device IDs**.
2. Select attributes from the Attributes list that you want to use to uniquely identify a device, and then click the right-arrow button to add the attribute to the Identity Attributes list. You can add as many attributes as you like.
3. Select the number of identity attributes (and hardware attributes) that a device must fail to match before it's designated as a duplicate of another device.
4. If you want the inventory scanner to reject duplicate device IDs, check the **Reject duplicate identities** option.
5. Click **OK** to save your settings and return to the **Configure Inventory** dialog.
6. (Optional) If you also want to resolve duplicate devices by name and/or address, click **Devices** to open the **Duplicate Devices** dialog where you can specify the conditions when duplicate devices are removed, such as when device names match, MAC addresses match, or both match.

About the Duplicate Device ID dialog

Use this dialog to set up duplicate device ID handling.

- **Attributes list:** Lists all of the attributes you can choose from to uniquely identify a device.
- **Identity attributes:** Displays the attributes you've selected to uniquely identify a device.
- **Duplicate device ID triggers:**
 - **Log as a duplicate device ID when:** Identifies the number of attributes that a device must fail to match before it's designated as a duplicate of another device.
- **Reject duplicate identities:** Causes the inventory scanner to record the device ID of the duplicate device and reject any subsequent attempts to scan that device ID. Then, the inventory scanner generates a new device ID.

About the Duplicate Devices dialog

Use this dialog to specify the name and/or address conditions when duplicate devices are removed from the database.

- **Remove duplicate when:**
 - **Device names match:** Removes the older record when two or more device names in the database match.
 - **MAC addresses match:** Removes the older record when two or more MAC addresses in the database match.
 - **Both device names and MAC addresses match:** Removes the older record ONLY when two or more device names and MAC addresses (for the same record) match.
- **Restore old device IDs:** Restores the original device ID from the older record of a scanned device, IF two records for that device exist in the database and at least one of the remove options above is selected and its criteria met, The original device ID is restored when the next inventory maintenance scan runs. This option has no affect unless one of the remove options above is selected.

Configuring the scheduler service

Use the **Scheduler** tab to configure the scheduler service (**Tools | Distribution | Scheduled tasks**) for the core server and database you selected using the **General** tab.

You must have the appropriate rights to perform these tasks, including full administrator privileges to the Windows NT/2000 devices on the network, allowing them to receive package distributions from the core server. You can specify multiple login credentials to use on devices by clicking **Change login**.

One additional setting you can configure manually is the **Scheduled task** window's refresh rate. By default, every two minutes the **Scheduled tasks** window checks the core database to determine if any of the visible items have been updated. If you want to change the refresh rate, navigate to this key in the registry:

```
HKEY_CURRENT_USER\Software\LANDesk\ManagementSuite\WinConsole
```

Set "TaskRefreshIntervalSeconds" to the number of seconds between refreshes for an active task. Set "TaskAutoRefreshIntervalSeconds" to the refresh interval for the whole **Scheduled task** window.

About the Configure Management Suite services dialog: Scheduler tab

Use this tab to see the name of the core server and the database that you selected earlier, and to specify the following scheduled task options:

- **Username:** The username under which the scheduled tasks service will be run. This can be changed by clicking the **Change login** button.
- **Number of seconds between retries:** When a scheduled task is configured with multiple retries, this setting controls the number of seconds the scheduler will wait before retrying the task.
- **Number of seconds to attempt wake up:** When a scheduled task is configured to use Wake On LAN, this setting controls the number of seconds that the scheduled tasks service will wait for a device to wake up.
- **Interval between query evaluations:** A number that indicates the amount of time between query evaluations, and a unit of measure for the number (minutes, hours, days, or weeks).
- **Wake on LAN settings:** The IP port that will be used by the Wake On LAN packet set by the scheduled tasks to wake up devices.
- **Schedule service status:** Indicates whether the service is started or stopped on the core server.
- **Start:** Starts the service on the core server.
- **Stop:** Stops the service on the core server.

About the Configure Management Suite services dialog: Change login dialog

Use the **Change login** dialog (click **Change login** on the **Scheduler** tab) to change the default scheduler login. You can also specify alternate credentials the scheduler service should try when it needs to execute a task on unmanaged devices.

To install LANDesk agents on unmanaged devices, the scheduler service needs to be able to connect to devices with an administrative account. The default account the scheduler service uses is LocalSystem. The LocalSystem credentials generally work for devices that aren't in a domain. If devices are in a domain, you must specify a domain administrator account.

If you want to change the scheduler service login credentials, you can specify a different domain-level administrative account to use on devices. If you're managing devices across multiple domains, you can add additional credentials the scheduler service can try. If you want to use an account other than LocalSystem for the scheduler service, or if you want to provide alternate credentials, you must specify a primary scheduler service login that has core server administrative rights. Alternate credentials don't require core server administrative rights, but they must have administrative rights on devices.

The scheduler service will try the default credentials and then use each credential you've specified in the **Alternate credentials** list until it's successful or runs out of credentials to try. Credentials you specify are securely encrypted and stored in the core server's registry.

You can set these options for the default scheduler credentials:

- **Username:** Enter the default domain\username or username you want the scheduler to use.
- **Password:** Enter the password for the credentials you specified.
- **Confirm password:** Retype the password to confirm it.

You can set these options for additional scheduler credentials:

- **Add:** Click to add the username and password you specified to the alternate credentials list.
- **Remove:** Click to remove the selected credentials from the list.
- **Modify:** Click to change the selected credentials.

When adding alternate credentials, specify the following:

- **Username:** Enter the username you want the scheduler to use.
- **Domain:** Enter the domain for the username you specified.
- **Password:** Enter the password for the credentials you specified.
- **Confirm password:** Retype the password to confirm it.

Configuring the custom jobs service

Use the **Custom jobs** tab to configure the custom jobs service for the core server and database you selected using the General tab. Examples of custom jobs include inventory scans, device deployments, or software distributions.

When you disable TCP remote execute as the remote execute protocol, custom jobs uses the standard LANDesk agent protocol by default, whether it's marked disabled or not. Also, if both TCP remote execute and standard LANDesk agent are enabled, custom jobs tries to use TCP remote execute first, and if it's not present, uses standard LANDesk agent remote execute.

The **Custom jobs** tab also enables you to choose options for device discovery. Before the custom jobs service can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

About the Configure Management Suite services dialog: Custom jobs tab

Use this tab to set the following custom jobs options:

Remote execute options

- **Disable TCP execute:** Disables TCP as the remote execute protocol, and thereby uses the standard LANDesk agent protocol by default.
- **Disable CBA execute / file transfer:** Disables standard LANDesk agent as the remote execute protocol. If standard LANDesk agent is disabled and TCP remote execute protocol is not found on the device, the remote execution will fail.
- **Enable remote execute timeout:** Enables a remote execute timeout and specifies the number of seconds after which the timeout will occur. Remote execute timeouts trigger when the device is sending heartbeats, but the job on the device is hung or in a loop. This setting applies to both protocols (TCP or standard LANDesk agent). This value can be between 300 seconds (5 minutes) and 86400 seconds (1 day).
- **Enable client timeout:** Enables a device timeout and specifies the number of seconds after which the timeout will occur. By default, TCP remote execute sends a heartbeat from device to server in intervals of 45 seconds until the remote execute completes or times out. Device timeouts trigger when the device doesn't send a heartbeat to the server.
- **Remote execute port (Default is 12174):** The port over which the TCP remote execute occurs. If this port is changed, it must also be changed in the device configuration.

Distribution option

- **Distribute to <nn> clients simultaneously:** The maximum number of devices to which the custom job will be distributed simultaneously.

Discovery options

- **UDP:** Selecting UDP uses a LANDesk agent ping via UDP. Most LANDesk device components depend on standard LANDesk agent, so your managed devices should have standard LANDesk agent on them. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping **Retries** and **Timeout**.

- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

Configuring the Multicast service

Use the **Multicast** tab to configure the multicast domain representative discovery options for the core server and database you selected using the **General** tab.

About the Configure Management Suite services dialog: Multicast tab

Use this tab to set the following multicast options:

- **Use multicast domain representative:** Uses the list of multicast domain representatives stored in the network view's **Configuration | Multicast domain representatives** group.
- **Use cached file:** Queries each multicast domain to find out who might already have the file, therefore not needing to download the file to a representative.
- **Use cached file before preferred domain representative:** Changes the order of discovery to make **Use cached file** the first option attempted.
- **Use broadcast:** Sends a subnet-directed broadcast to find any device in that subnet that could be a multicast domain representative.
- **Log discard period (days):** Specifies the number of days that entries in the log will be retained before being deleted.

Configuring the OS deployment service

Use the **OS deployment** tab to designate PXE representatives as PXE holding queues, and to configure basic PXE boot options for the core server and database you selected using the **General** tab.

PXE holding queues are one method of deploying OS images to PXE-enabled devices. You designate existing PXE representatives (located in the **Configuration** group in the network view) as PXE holding queues. For more information, see PXE-based deployment.

Select and move PXE representatives from the **Available proxies** list to the **Holding queue proxies** list.

About the Configure Management Suite Services dialog: OS Deployment tab

Use this tab to assign PXE holding queue proxies (representatives), and to specify the PXE boot options.

- **Available proxies:** Lists all available PXE proxies on your network, identified by device name. This list is generated when the inventory scanner detects PXE software (PXE and MTFTP protocols) running on the device.
- **Holding queue proxies:** Lists the PXE proxies that have been moved from the **Available proxies** list, thereby designating the proxy as a PXE holding queue. PXE-enabled devices on the same subnet as the PXE holding queue proxy will be automatically added to the **PXE holding queue** group in the console's network view when they PXE boot. The devices can then be scheduled for an image deployment job.
- **Reset:** Forces all of the PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the **PXE holding queue** group in the console's network view. The devices can then be scheduled for an imaging job. (The Reset button is enabled when you select a PXE proxy in the Holding queue proxies list.)
- **PXE boot options:** Determines how the PXE boot prompt operates when devices attempt to PXE boot.

Note: Changes you make here to the PXE boot options will not take effect on any of your PXE representatives until you run the PXE Representative Deployment script on that representative.

- **Timeout:** Indicates how long the boot prompt displays before timing out and resuming the default boot process. The maximum number of seconds you can enter is 60 seconds.
- **Message:** Specifies the PXE boot prompt message that appears on the device. You can type any message you like in the text box, up to 75 characters in length.

Configuring device agents

Devices need the Management Suite agents on them to be fully manageable. Read this chapter to learn about:

- Working with agent configurations
- Creating an agent configuration
- Updating agent preferences on devices
- Creating standalone agent configuration packages
- Agent security and trusted certificates
- Uninstalling device agents

The **Agent configuration** window lets you create new agent configurations for Windows, Linux, and Macintosh devices. The agent configurations you create can then be pushed to clients using the console's **Scheduled tasks** window.

Creating device configurations for Windows NT/2000/2003/XP devices not enabled for management

If you have Windows NT/2000/2003/XP devices that are part of a Windows NT/2000/2003/XP domain, you can push a configuration to those devices even if the CBA and Remote Control agents are not present. For more information, see the *Installation and Deployment Guide*.

Working with agent configurations

Management Suite uses agent configurations that you create to deploy agents and agent preferences to managed devices. Once devices have the Management Suite agents on them, you can easily update agent configurations. For more information on initial agent deployment, see the "Deploying the primary agents to clients" chapter in the *Installation and Deployment Guide*.

Read the following section for more information on:

- Agent configuration changes in Management Suite 8.5
- Creating an agent configuration
- Updating agent preferences on devices
- Creating standalone agent configuration packages

Agent configuration changes in Management Suite 8.5+

Users of Management Suite prior to version 8.5 will notice several agent configuration changes from past releases.

- The standard LANDesk agent is the new name for CBA and it now includes the inventory scanner, local scheduler, patch management, software monitoring, and bandwidth detection. These components aren't individually selectable and are installed by default. You can also set reboot options in the standard LANDesk agent.
- Application policy management is now called policy-based delivery and it's configured under software distribution.
- Targeted Multicast is supported by software distribution. You don't need to separately enable it or configure it.
- The security and patch scanner agent is now installed by default with the standard LANDesk agent. You can configure this agent to determine how and when the security and patch scanner runs on devices and whether to show progress on the end user device. (Even without a LANDesk Security Suite content subscription, the security scanner allows you to check for LANDesk software updates on devices and core servers. With a subscription, you can take full advantage of the scanner's capability to scan for and remediate known vulnerabilities, spyware, and other potential security risks.)

Creating an agent configuration

Use the **Agent configuration** window to create and update device and server agent configurations (such as what agents are installed on devices and what network protocols the agents use).

You can create different configurations for groups' specific needs. For example, you could create configurations for the devices in your accounting department or for devices using a particular operating system.

To push a configuration to devices, you need to:

- **Create the agent configuration:** Set up specific configurations for your devices.

- **Schedule the agent configuration:** Push the configuration to devices that have the standard LANDesk agent installed. For more information, see "Scheduling tasks." Users with administrative rights can also install the default agent configuration by running WSCFG32.EXE or IPSETUP.BAT from the core server's LDLogon share.

To create an agent configuration

1. In the console, click **Tools | Configuration | Agent configuration**.
2. Click the **New** toolbar button.
3. Enter a **Configuration name**.
4. In the **Agent configuration** window's **Start** page, select the agents you want to deploy.
5. Use the tree to navigate the dialogs relating to the options you selected. Customize the options you selected as necessary. Click **Help** for more information if you have questions about a page.
6. Click **Save & Close**.
7. If you want the configuration to be the default (the configuration LDLOGON\WSCFG32.EXE or LDLOGON\IPSETUP.BAT will install), from the configuration's shortcut menu, click **Default configuration**.

For more information on device setup options, see the device setup help topic and the *Installation and Deployment Guide*.

Using the advance agent

The advance agent reduces the amount of network bandwidth used for Windows-based agent configuration. The advance agent works well with any type of device, including mobile devices with intermittent or slow network connections.

The advance agent is a small 500 KB .MSI package. When this package runs on a managed device, it downloads an associated full agent configuration package, which may be up to 15 MB in size, depending on the agents you select. In the **Advance agent configuration** dialog, you can configure what bandwidth-friendly distribution options the .MSI will use for the full agent configuration download.

The advance agent works independently from the core server once it starts downloading the full agent configuration. If a device disconnects from the network before the agent configuration finishes downloading, the advance agent will automatically resume the download once the device is back on the network.

When you create an advance agent configuration, it takes a few seconds for the console to create the full agent configuration package. The console places the advance agent package (<configuration name>.msi) and the newly-created full agent configuration package (<configuration name>.exe) in the core server's LDLogon\AdvanceAgent folder. The file names are based on the agent configuration name.

Once you've created an agent configuration package, you need to run the .MSI portion on devices by using one of the following methods:

- Schedule the small .MSI portion for push distribution.
- Run the .MSI manually on each device.
- Manually configure the .MSI to run via a login script.

Once you deploy the advance agent to devices, the advance agent starts downloading the associated agent configuration. The agent runs silently on the managed device, without showing any dialogs or status updates. The advance agent uses the bandwidth preferences you specified in the **Advance agent configuration** dialog, such as Peer Download and dynamic bandwidth throttling.

Once the .MSI installs and successfully configures agents on a device, it removes the full agent configuration package. The .MSI portion stays on the device and if the same .MSI runs again it won't reinstall the agents.

To create an advance agent configuration

1. Create a Windows-based agent configuration (**Tools | Configuration | Agent configuration**).
2. From that configuration's shortcut menu, click **Advance agent**.
3. Select the options you want.
4. If you'll be relocating the associated agent configuration package (the .EXE file), change the path for the agent configuration package to match the new location.
5. Click **OK**.
6. If necessary, copy the associated .EXE file from the LDLogon\AdvanceAgent folder to your distribution server. Make sure the path to the agent configuration executable matches the path you specified in the **Advance agent configuration** dialog. You should leave the MSI package on the core server in the default location. Otherwise, the package won't be visible for the advance agent push distribution task below.

To set up an advance agent push distribution

1. In the Agent configuration window (**Tools | Configuration | Agent configuration**), click the **Schedule a push of an advance agent configuration** button.
2. The **Advance agent configurations** dialog lists the agent configurations in the LDLogon\AdvanceAgent folder. Click the configuration you want to distribute and click **OK**.
3. The **Scheduled tasks** window opens with the advance agent task you created selected. The task name is "Advance agent <your configuration name>".
4. Add target devices to the task by dragging them from the **Network view** and dropping them on the task in the **Scheduled tasks** window.
5. From the task's shortcut menu, click **Properties** and schedule the task. You can see the .MSI portion distribution progress in the **Scheduled tasks** window. There are no status updates on the full agent configuration once the .MSI distribution completes.

Updating agent preferences on devices

If you want to update agent preferences on devices, such as requiring permission for remote control, you don't have to redeploy the entire agent configuration. You can make the changes you want in the **Agent configuration** window, and from that configuration's shortcut menu click **Schedule update**. This opens the **Scheduled tasks** window and creates an update task and package for the configuration you scheduled the update from. This package is only a few hundred kilobytes in size.

Note that updating preferences won't install or remove agents on a device. If the update contains preferences for agents that aren't on a device, the preferences that don't apply will be ignored.

To update agent preferences on devices

1. Click **Tools | Configuration | Agent configuration**.

2. Customize the configuration you want to use.
3. When you're done, from the configuration's shortcut menu, click **Schedule update**. This opens the **Scheduled tasks** window.
4. Target the devices you want to update and schedule the task.

Creating standalone agent configuration packages

Normally the client configuration utility, WSCFG32.EXE, configures clients. If you want, you can have the **Agent configuration** window create a self-extracting single-file executable that installs an agent configuration on the device it's run on. This is helpful if you want to install agents from a CD or portable USB drive, or if you want to multicast an agent configuration.

To create a standalone agent configuration package

1. Click **Tools | Configuration | Agent configuration**.
2. Customize the configuration you want to use.
3. When you're done, from the configuration's shortcut menu, click **Create self-contained client installation package**.
4. Select the path where you want the package stored.
5. Wait for Management Suite to create the package. It may take a few minutes.

Agent security and trusted certificates

With Management Suite 8, the certificate-based authentication model has been simplified. Device agents still authenticate to authorized core servers, preventing unauthorized cores from accessing clients. However, Management Suite 8 doesn't require a separate certificate authority to manage certificates for the core, console, and each client. Instead, each core server has a unique certificate and private key that Management Suite Setup creates when you first install the core or rollup core server.

These are the private key and certificate files:

- **<keyname>.key:** The .KEY file is the private key for the core server, and it only resides on the core server. If this key is compromised, the core server and device communications won't be secure. Keep this key secure. For example, don't use e-mail to move it around.
- **<keyname>.crt:** The .CRT file contains the public key for the core server. The .CRT file is a viewer-friendly version of the public key that you can view to see more information about the key.
- **<hash>.0:** The .0 file is a trusted certificate file and has content identical to the .CRT file. However, it's named in a manner that lets the computer quickly find the certificate file in a directory that contains many different certificates. The name is a hash (checksum) of the certificates subject information. To determine the hash filename for a particular certificate, view the <keyname>.CRT file. There is a .INI file section [LDMS] in the file. The hash=value pair indicates the <hash> value.

An alternate method for getting the hash is to use the openssl application, which is stored in the \Program Files\LANDesk\Shared Files\Keys directory. It will display the hash associated with a certificate using the following command line:

```
openssl.exe x509 -in <keyname>.crt -hash -noout
```

All keys are stored on the core server in \Program Files\LANDesk\Shared Files\Keys. The <hash>.0 public key is also in the LDLOGON directory and needs to be there by default. <keyname> is the certificate name you provided during Management Suite Setup. During Setup, it's helpful to provide a descriptive key name, such as the core server's name (or even its fully qualified name) as the key name (example: Idcore or Idcore.org.com). This will make it easier to identify the certificate/private key files in a multi-core environment.

You should back up the contents of your core server's Keys directory in a safe, secure place. If for some reason you need to reinstall or replace your core server, you won't be able to manage that core server's devices until you add the original core's certificates to the new core, as described below.

Sharing keys among core servers

Devices will only communicate with core and rollup core servers for which they have a matching trusted certificate file. For example, let's say you have three core servers, managing 5,000 devices each. You also have a rollup core managing all 15,000 devices. Each core server will have its own certificate and private keys, and by default, the device agents you deploy from each core server will only talk to the core server from which the device software is deployed.

There are two main ways of sharing keys among core and rollup core servers:

1. Distributing each core server trusted certificate (the <hash>.0 file) to devices and their respective core servers. This is the most secure way.

2. Copying the private key and certificates to each core server. This doesn't require you to do anything to devices, but since you have to copy the private key, it exposes more risk.

In our example, if you want the rollup core and Web console to be able to manage devices from all three cores, you need to distribute the rollup core's trusted certificate (the <hash>.0 file) to all devices, in addition to copying the same file to each core server's LDLOGON directory. For more information, see "Distributing trusted certificates to devices" in the next section.

Alternatively, you can copy the certificate/private key files from each of the three core servers to the rollup core. This way, each device can find the matching private key for its core server on the rollup core server. For more information, see "Copying certificates/private key files among core servers" later in this chapter.

If you want one core to be able to manage devices from another core, you can follow the same process, either distributing the trusted certificate to devices or copying the certificate/public key files among cores.

If you are copying certificates between standalone cores (not to a rollup core), there is an additional issue. A core won't be able to manage another core's devices unless it first has an inventory scan from those devices. One way of getting inventory scans to another core is to schedule an inventory scan job with a custom command line that forwards the scan to the new core. In a multiple core scenario, using a rollup core and the Web console is a simpler way to manage devices across cores. Rollup cores automatically get inventory scan data from all devices on the cores that get rolled up to it.

Distributing trusted certificates to devices

There are two ways you can deploy trusted certificates to devices:

1. Deploy a device setup configuration that includes the core server trusted certificates you want.
2. Use a software distribution job to directly copy the trusted certificate files you want to each device.

Each additional core server trusted certificate (<hash>.0) that you want devices to use must be copied to the core server's LDLOGON directory. Once the trusted certificate is in this directory, you can select it within the device setup dialog's **Common base agent** page. Device setup copies keys to this directory on devices:

- Windows devices: \Program Files\LANDesk\Shared Files\cbaroot\certs
- Mac OS X devices: /usr/LANDesk/common/cbaroot/certs

If you want to add a core server's certificate to a device, and you don't want to redeploy device agents through device setup, create a software distribution job that copies < hash>.0 to the directory specified above on the device. You can then use the **Scheduled tasks** window to deploy the certificate distribution script you created.

The following is an example of a custom script that can be used to copy a trusted certificate from the LDLOGON directory of the core server to a device. To use this, replace d960e680 with the hash value for the trusted certificate you want to deploy.

```
; Copy a trusted certificate from the ldlogon directory of the core
server
; into the trusted certificate directory of the client
[MACHINES]
REMCOPY0=%DTMDIR%\ldlogon\d960e680.0, %TRUSTED_CERT_PATH%\d960e680.0
```

Copying certificate/private key files among core servers

An alternative to deploying certificates (<hash>.0) to devices is to copy certificate/private key sets among cores. Cores can contain multiple certificate/private key files. As long as a device can authenticate with one of the keys on a core, it can communicate with that core.

When using certificate-based remote control, target devices must be in the core database

If you're using certificate-based remote control security with devices, you can only remote control devices that have an inventory record in the core database that you're connected to. Before contacting a node to launch remote control, the core looks in the database to ensure the requesting party has the right to view the device. If the device isn't in the database, the core denied the request.

To copy a certificate/private key set from one core server to another

1. At the source core server, go to the \Program Files\LANDesk\Shared Files\Keys folder.
2. Copy the source server's <keyname>.key, <keyname>.crt, and <hash>.0 files to a floppy disk or other secure place.
3. At the destination core server, copy the files from the source core server to the same folder (\Program Files\LANDesk\Shared Files\Keys). The keys take effect immediately.

Care should be taken to make sure that the private key <keyname>.key is not compromised. The core server uses this file to authenticate devices, and any computer with the <keyname>.key file can perform remote executions and file transfer to a Management Suite device.

Uninstalling device agents

Prior to Management Suite 8.5, anyone could uninstall Management Suite agents by running WSCFG32 with the /u parameter. Since WSCFG32 was in the LDLogon share, which managed devices could access, it was relatively easy for users to uninstall Management Suite agents.

With Management Suite 8.5 and later, the /u parameter has been removed from WSCFG32. There's a new utility called UninstallWinClient.exe in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Management Suite or Server Manager agents on any device it runs on. You can move it to any folder you want or add it to a login script. It's a Windows application that runs silently without displaying an interface.

Running this program won't remove a device from the core database. If you redeploy agents to a device that ran this program, it will be stored in the database as a new device.

Using LANDesk Server Manager and LANDesk System Manager with LANDesk Management Suite

Server Manager and System Manager are available separately from LANDesk Software and integrate with Management Suite. Management Suite includes one server license and as many device licenses as you purchased. If you install Management Suite agents on a server operating system, Management Suite requires an additional server license for each server. Server Manager adds Management Suite server licenses, in addition to Server Manager-specific features for managed servers.

System Manager helps you manage devices on your network and troubleshoot common computer problems before they become serious. If you have devices on your network that you're already managing with System Manager, you can use Management Suite's System Manager integration to manage these computers from the Management Suite console.

Management Suite works with some versions of Linux and UNIX. These features of Management Suite are supported for Linux and UNIX computers:

- Software distribution.
- Inventory scanning for hardware and software.
- Queries from the management console on any attribute that the inventory scanner reports to the core database.
- Security Suite vulnerability scanning. Remediation isn't supported at this time.

System requirements

Linux runs on a variety of architectures, but the Linux inventory scanner will only run on Intel architecture.

Supported Linux and UNIX distributions:

- Red Hat Linux 7.3, 8.0, and 9.0
- IBM AIX 5.1
- Intel Architecture Solaris 8
- Sun Sparc (Solaris 8)
- HP-UX 11.0

Installing Linux server agents

You can remotely deploy and install Linux agents and RPMs on Linux servers. Your Linux server must be configured correctly for this to work. To install an agent on a Linux server, you must have root privileges.

The default Red Hat Enterprise 3 Linux AS and ES install includes the RPMs that the Linux standard agent requires. If you select the monitoring agent in **Configure agents**, you need two additional RPMs, perl-CGI and sysstat. For the complete list of RPMs that the product requires, see the *Installation and Deployment Guide*.

For an initial Linux agent configuration, the core server uses an SSH connection to target Linux servers. You must have a working SSH connection with username/password authentication. This product doesn't support public key/private key authentication. Any firewalls between the core and Linux servers need to allow the SSH port. Consider testing your SSH connection from the core server with a 3rd-party SSH application.

The Linux agent installation package consists of a shell script, agent tarballs, .INI agent configuration, and agent authentication certificates. These files are stored in the core server's LDLogon share. The shell script extracts files from the tarballs, installs the RPMs, and configures the server to load the agents and run the inventory scanner periodically at the interval you specified in the agent configuration. Files are placed under /usr/LANDesk.

Use the Configure services utility to enter the SSH credentials you want the scheduler service to use as alternate credentials. The scheduler service uses these credentials to install the agents on your servers. You should be prompted to restart the scheduler service. If you aren't, click **Stop** and then **Start** on the **Scheduler** tab to restart the service. This activates your changes.

Deploying the Linux agents

After you've configured your Linux servers and added Linux credentials to the core server, you must create a Linux agent configuration, and then use unmanaged device discovery to discover your Linux servers. You can then add the discovered servers to the **My devices** list so you can deploy the Linux agents. Before you can deploy to a server, you must add it to the **My devices** list. Do this by discovering your Linux server with unmanaged device discovery.

To create a Linux agent configuration

1. In **Tools | Configuration | Agent configuration**, click the **New Linux** button.
2. Enter a **Configuration name**.
3. On the **Start** page, the Standard LANDesk agent, remote control, and software distribution agents are installed by default. If you want to install the **LANDesk vulnerability scanner**, check that box.
4. On the **Standard LANDesk agent** page, select the **Trusted certificates for agent authentication** that you want installed. For more information, see Agent security and trusted certificates.
5. Click **Save**.

To discover your Linux servers and deploy a configuration to them

1. In **Tools | Configuration | Unmanaged Device discovery**, create a discovery job for each Linux server. Use a standard network scan and enter the Linux server's IP address for the starting and ending IP ranges. If you have many Linux servers, enter a range of IP addresses. Click **Scan now** once you've added your discovery IP ranges.

2. When the task finishes, verify that unmanaged device discovery found the Linux servers you want to manage.
3. In the **Unmanaged device discovery** window, drag the Linux servers onto the Linux configuration that you want in the **Agent configuration** window.
4. Finish scheduling the task in the **Scheduled tasks** window.

Manually installing the Linux agents

To pull a Linux agent configuration

1. Copy the following files from the LDLOGON share:

*.0 (the "dot zero" files are the certificates for the Common !CompanyName! Agent - there should be one .0 file)

<configuration name>.sh (substitute your configuration name here)

unix\linux\baseclient.tar.gz

unix\linux\monitoring.tar.gz

unix\linux\vulscan.tar.gz

2. Place the files on the Linux box you are to pull from in a temporary directory, such as "/tmp/ldcfg".
3. If the machine is an IPMI/BMC machine (with Monitoring included in the installation), type the following on a command line:

```
export BMCPW="(bmc password) "
```

4. Running as root, execute the shell script for the configuration. For example, if you named the script "basic-linux," use the full path used in step 2:

```
/tmp/ldcfg/basic-linux.sh
```

Inventory scanner command-line parameters

The inventory scanner, `ldiscnux`, has several command-line parameters that specify how it should run. See "`ldiscnux -h`" or "`man ldiscnux`" for a detailed description of each. Each option can be preceded by either '-' or '/'.

Parameter	Description
-d=Dir	Starts the software scan in the Dir directory instead of the root. By default, the scan starts in the root directory.
-f	Forces a software scan. If you don't specify -f, the scanner does software scans on the day interval (every day by default) specified in the console under Configure Services Inventory Scanner Settings .
-f-	Disables the software scan.
-i=ConfName	Specifies the configuration filename. Default is <code>/etc/ldappl.conf</code> .
-ntt=address:port	Host name or IP address of core server. Port is optional.

-o=File	Writes inventory information to the specified output file.
-s=Server	Specifies the core server. This command is optional, and only exists for backward compatibility.
-stdout	Writes inventory information to the standard output.
-v	Enables verbose status messages during the scan.
-h or -?	Displays the help screen.

Examples

To output data to a text file, type:

```
ldiscnux -o=data.out -v
```

To send data to the core server, type:

```
ldiscnux -ntt=ServerIPName -v
```

Linux inventory scanner files

File	Description
ldiscnux	<p>The executable that is run with command-line parameters to indicate the action to take. All users that will run the scanner need sufficient rights to execute the file.</p> <p>There is a different version of this file for each platform supported above.</p>
/etc/ldiscnux.conf	<p>This file always resides in /etc and contains the following information:</p> <ul style="list-style-type: none"> • Inventory assigned unique ID • Last hardware scan • Last software scan <p>All users who run the scanner need read and write attributes for this file. The unique ID in /etc/ldiscnux.conf is a unique number assigned to a computer the first time the inventory scanner runs. This number is used to identify the computer. If it ever changes, the core server will treat it as a different computer, which could result in a duplicate entry in the database.</p> <p>Warning: Do not change the unique ID number or remove the ldiscnux.conf file after it has been created.</p>
/etc/ldappl.conf	<p>This file is where you customize the list of executables that the inventory scanner will report when running a software scan. The file includes some examples, and you'll need to add entries for software packages that you use. The search criteria are based on filename and file size. Though this file will typically reside in /etc, the scanner can use an alternative file by using the -i= command-line parameter.</p>
ldiscnux.8	Man page for ldiscnux.

Console integration

Once a Linux computer is scanned into the core database, you can:

- Query on any of the attributes returned by the Linux inventory scanner to the core database.
- Use the reporting features to generate reports that include information that the Linux scanner gathers. For example, Linux will appear as an OS type in the Operating Systems Summary Report.
- View inventory information for Linux computers.

Queries on "System Uptime" sort alphabetically, returning unexpected results

If you want to do a query to find out how many computers have been running longer than a certain number of days (for example, 10 days), query on "System Start" rather than "System Uptime." Queries on System Uptime may return unexpected results, because the system uptime is simply a string formatted as "x days, y hours, z minutes, and j seconds." Sorting is done alphabetically and not on time intervals.

Path to config files referenced in `ldappl.conf` doesn't appear in the console

ConfFile entries in `ldappl.conf` file need to include a path.

Required RPMs (version # or later)

It is recommended that you store all RPMs in the `...ManagementSuite\ldlogon\RPMS` directory. You can browse to this folder through `http://core name/RPMS`.

REDHAT ENTERPRISE

perl

RPM Version:5.8.0-88.4

Binary Version:5.8.0

python

RPM Version:2.2.3-5

Binary Version:2.2.3

pygtk2

RPM Version:1.99.16-8

Binary Version:

sudo

RPM Version:1.6.7p5-1

Binary Version:1.6.7.p5

bash

RPM Version:2.05b-29

Binary Version:2.05b.0(1)-release

xinetd

RPM Version:2.3.12-2.3E

Binary Version:2.3.12

mozilla

RPM Version:

Binary Version:1.5

openssl

RPM Version:0.9.7a-22.1

Binary Version:0.9.7a

perl-CGI

RPM Version:2.81-88.4

Binary Version:2.81-88.4

perl-Filter

RPM Version:1.29-3

Binary Version:1.06

sysstat

RPM Version:4.0.7-4

Binary Version:4.0.7

SUSE LINUX

(SuSE 64)

bash

RPM Version: 2.05b-305.6

mozilla

RPM Version: 1.6-74.14

mysql

RPM Version: 4.0.18-32.9

mysql-server

RPM Version: NA [provided by mysql]

net-snmp

RPM Version: 5.1-80.9

openssl

RPM Version: 0.9.7d-15.13

perl

RPM Version: 5.8.3-32.1

perl-CGI

RPM Version: NA [provided by perl]

perl-DBD

RPM Version: mysql-2.9003-22.1 [note: case change]

perl-DBI

RPM Version: 1.41-28.1

perl-Filter

RPM Version: NA [provided by perl]

python-gtk

RPM Version: 2.0.0-215.1 [note: package name change]

python

RPM Version: 2.3.3-88.1

sudo

RPM Version: 1.6.7p5-117.1

sysstat

RPM Version: 5.0.1-35.1

xinetd

RPM Version: 2.3.13-39.3

lm_sensors

RPM Version: NA (note: this has been incorporated into the kernel for the 2.6 version)

Using database queries

Queries are customized searches for managed devices. LANDesk Management Suite provides a method for you to query devices that have been scanned into your core database via database queries, as well as a method for you to query for devices located in other directories via LDAP queries. You view, create and organize database queries with the Queries groups in the console's network view. You create LDAP queries with the Directory Manager tool.

For more information on creating and using LDAP directory queries with Directory Manager, see [Using LDAP queries](#).

Read this chapter to learn about:

- [Queries overview](#)
- [Query groups](#)
- [Creating database queries](#)
- [Running queries](#)
- [Importing and exporting queries](#)

Queries overview

Queries help you manage your network by allowing you to search for and organize network devices that are in the core database, based on specific system or user criteria.

For example, you can create and run a query that captures only devices with a processor clock speed of less than 166 MHz, or with less than 64 MB of RAM, or a hard drive of less than 2 GB. Create one or more query statements that represent those conditions and relate statements to each other using standard logical operators. When the queries are run, you can print the results of the query, and access and manage the matching devices.

Query groups

Queries can be organized into groups in the network view. Create new queries (and new query groups) by right-clicking either the **My queries** group and selecting **New query** or **New group**, respectively.

A Management Suite administrator (user with LANDesk Administrator rights) can view the contents of all of the query groups, including: **My queries**, **Public queries**, **All queries**, and **User queries**.

When other Management Suite users log in to the console, they can see queries in the **My queries**, **Public queries**, and **All queries** groups, based on their device scope. A user will not see the **User queries** group.

When you move a query to a group (by right-clicking and selecting **Add to new group** or **Add to existing group**, or by dragging and dropping the query), you're actually creating a copy of the query. You can remove the copy in any query group and the master copy of the query (in the **All queries** group) isn't affected. If you want to delete the master copy, you can do it from the **All Queries** group.

For more information on how query groups and queries display in the network view, and what you can do with them, see "Understanding the network view."

Creating database queries

Use the **New query** dialog to build a query by selecting from attributes, relational operators, and the attribute's values. Build a query statement by choosing an inventory attribute and relating it to an acceptable value. Logically relate the query statements to each other to ensure they're evaluated as a group before relating them to other statements or groups.

To create a database query

1. In the console's network view, right-click the **My queries** group (or **Public queries**, if you have the public query management right), and then click **New query**.
2. Enter a unique name for the query.
3. Select a component from the inventory attributes list.
4. Select a relational operator.
5. Select a value from the values list. You can edit a value.
6. Click **Insert** to add the statement to the query list.
7. If you want to query for more than one component, click a logical operator (AND, OR) and repeat steps 2-5.
8. (Optional) To group query statements so they're evaluated as a group, select two or more query statements and click **Group()**.
9. When you're finished adding statements, click **Save**.

About the New query dialog

Use this dialog to create a new query with the following functions:

- **Name:** Identifies the query in query groups.
- **Machine components:** Lists inventory components and attributes the query can scan for.
- **Relational operators:** Lists relational operators. These operators determine which description values for a certain component will satisfy the query.

The Like operator is a new relational operator. If a user doesn't specify any wild cards (*) in their query, the Like operator adds wildcards to both ends of the string. Here are three examples of using the Like operator:

Computer.Display Name LIKE "Bob's Machine" queries for: Computer.Display Name LIKE "%Bob's Machine%"

Computer.Display Name LIKE "Bob's Machine*" queries for: Computer.Display Name LIKE "Bob's Machine%"

Computer.Display Name LIKE "*Bob's Machine" queries for: Computer.Display Name LIKE "%Bob's Machine"

- **Display scanned values:** Lists acceptable values for the chosen inventory attribute. You can also manually enter an appropriate value, or edit a selected value, with the Edit values field. If the selected relational operator is Exists or Does Not Exist, no description values are possible.
- **Logical operator:** Determines how query statements logically relate to each other:
 - **AND:** Both the previous query statement AND the statement to be inserted must be true to satisfy the query.
 - **OR:** Either the previous query statement OR the statement to be inserted must be true to satisfy the query.

- **Insert:** Inserts the new statement into the query list and logically relates it to the other statements according to the listed logical operator. You can't choose this button until you've built an acceptable query statement.
- **Edit:** Lets you edit the selected query statement. When you're finished making changes, click the **Update** button.
- **Delete:** Deletes the selected statement from the query list.
- **Clear all:** Deletes all statements from the query list.
- **Query list:** Lists each statement inserted into the query and its logical relationship to the other listed statements. Grouped statements are surrounded by parentheses.
- **Group ():** Groups the selected statements together so they're evaluated against each other before being evaluated against other statements.
- **Ungroup:** Ungroups the selected grouped statements.
- **Filters:** Opens the Query Filter dialog that displays device groups. By selecting device groups, you limit the query to only those devices contained in the selected groups. If you don't select any groups, the query ignores group membership.
- **Select columns:** Lets you add and remove columns that appear in the query results list for this query. Select a component, and then click the right-arrow button to add it to the column list. You can manually edit the Alias and Sort Order text, and your changes will appear in the query results list.
- **Qualifier:** The qualifier button is used to limit the results of one-to-many relationships in the database; without it, you will get the same machine listed numerous times in your result set. For example, if you want to see which version of Microsoft Word is installed on every machine in your organization, you would insert Computer.Software.Package.Name = "Microsoft Word" in the query box and select Computer.Software.Package.Version in the Select Columns list. However, simply listing the software version will list every version of every piece of software installed on each machine; precisely what you don't want. The solution is to limit (or qualify) the version to only Microsoft Word. Click on the Qualify button and you will be able to insert Computer.Software.Package.Name = "Microsoft Word". This will return only the versions of Microsoft Word.
- **Save:** Saves the current query. When you save a query before running it, the query is stored in the core database and remains there until you explicitly delete it.

Query statements are executed in the order shown

If no groupings are made, the query statements listed in this dialog are executed in order from the bottom up. Be sure to group related query items so they're evaluated as a group; otherwise, the results of your query may be different than you expect.

Running database queries

To run a query

1. In the network view, expand the query groups to locate the query you want to run.
2. Double-click the query. Or, right-click and select **Run**.
3. The results (matching devices) display in the right-hand pane of the network view.

Importing and exporting queries

You can use import and export to transfer queries from one core database to another. You can import:

- Management Suite 8 exported queries
- Web console exported .XML queries
- Management Suite 6.52, 6.62, and 7.0 exported .QRY queries

To import a query

1. Right-click the query group where you want to place the imported query.
2. Select **Import** from the shortcut menu.
3. Navigate to the query you want to import and select it.
4. Click **Open** to add the query to the selected query group in the network view.

To export a query

1. Right-click the query you want to export.
2. Select **Export** from the shortcut menu.
3. Navigate to the location where you want to save the query (as an .XML file).
4. Type a name for the query.
5. Click **Save** to export the query.

Using LDAP queries

In addition to the ability to query the core database with database queries, Management Suite also provides the Directory Manager tool that lets you locate, access, and manage devices in other directories via LDAP (the Lightweight Directory Access Protocol).

You can query devices based on specific attributes such as processor type or OS. You can also query based on specific user attributes such as employee ID or department.

For information about creating and running database queries from the Queries groups in the network view, see "Using database queries."

Read this chapter to learn about:

- About the Directory Manager window
- Creating LDAP directory queries
- More about LDAP

About the Directory manager window

Use directory manager to accomplish the following tasks:

- **Manage directory:** Opens the **Directory properties** dialog where you identify and log in to an LDAP directory.
- **Remove directory:** Removes the selected directory from the preview pane and stops managing it.
- **Refresh view:** Reloads the list of managed directories and targeted users.
- **New query:** Opens the **LDAP query** dialog where you can create and save an LDAP query.
- **Delete query:** Deletes the selected query.
- **Run query:** Generates the results of the selected query.
- **Object properties:** See the properties for the selected object.

Using directory manager, you can drag LDAP groups and saved LDAP queries onto scheduled tasks, making them task targets.

The directory manager window consists of two panes: a directory pane on the left and a preview pane on the right.

Directory pane

The directory pane displays all registered directories and users. As an administrator, you can specify the name of a registered directory and see a list of queries that are associated with the directory. You can create and then save new queries for a registered directory with a right mouse click or by using drop-down menus. After creating a query, you can drag and drop it to the **Scheduled tasks** window so that the task is applied to users who match the query.

Preview pane

When you select a saved query in directory manager's directory pane on the left side of the dialog, the policies targeted to that query appear in the preview pane on the right side. Likewise, when an individual LDAP user is selected in the directory pane, the policies targeted to that user appear in the preview pane.

- **Registered directory:** Query groups item and Browse item.
- **Query groups:** Queries associated with the directory.
- **Query:** Provides details about the query.
- **Browse and directory items:** Sub-items in the directory.

Creating LDAP directory queries

To create and save a directory query

The task of creating a query for a directory and saving that query is divided into two procedures:

To select an object in the LDAP directory and initiate a new query

1. Click **Tools | Distribution | Directory Manager**.

2. Browse the **Directory Manager** directory pane, and select an object in the LDAP directory. You'll create an LDAP query that returns results from this point in the directory tree down.
3. From directory manager, click the **New query** toolbar button. Note that this icon only appears when you select the root organization (o) of the directory tree (o=my company) or an organizational unit (ou=engineering) within the root organization. Otherwise, it's dimmed.
4. The **Basic LDAP query** dialog appears.

To create, test, and save the query

1. From the **Basic LDAP query** dialog, click an attribute that will be a criterion for the query from the list of directory attributes (example = department).
2. Click a comparison operator for the query (=, <=, >=).
3. Enter a value for the attribute (example department = engineering).
4. To create a complex query that combines multiple attributes, select a combination operator (AND or OR) and repeat steps 1 through 3 as many times as you want.
5. When you finish creating the query, click **Insert**.
6. To test the completed query, click **Test query**.
7. To save the query, click **Save**. The saved query will appear by name under **Saved queries** in the directory pane of directory manager.

About the Basic LDAP query dialog

- **LDAP query root:** Select a root object in the directory for this query (LDAP://ldap.xyzcompany.com/ou = America.o = xyzcompany). The query that you're creating will return results from this point in the tree down.
- **LDAP attributes:** Select attributes for user-type objects.
- **Operator:** Select the type of operation to perform relating to an LDAP object, its attributes, and attribute values including equal to (=), less than or equal to (<=), and greater than or equal to (>=).
- **Value:** Specify the value assigned to the attribute of an LDAP object.
- **AND/OR/NOT:** Boolean operators that you can select for your query conditions.
- **Test query:** Execute a test of the query you've created.
- **Save:** Save the created query by name.
- **Advanced:** Create a query using the elements of a basic LDAP query but in a freeform manner.
- **Insert:** Insert a line of query criteria.
- **Delete:** Delete a selected line of criteria.
- **Clear all:** Clear all lines of query criteria.

About the Save LDAP query dialog

From the **Basic LDAP query** dialog, click **Save** to open the **Save LDAP query** dialog, which displays the following:

- **Choose a name for this query:** Enables you to choose a name for the query you've created.
- **Query Details LDAP Root:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Query Details LDAP Query:** Displays query examples you can use as a guide when creating your own query in freeform.

- **Save:** Enables you to save the created query by name. The query is saved under the **Saved queries** item under the LDAP directory entry in the directory manager directory pane.

About the Directory properties dialog

From the directory manager toolbar, click the **Manage directory** toolbar button to open the **Directory properties** dialog. This dialog enables you to start managing a new directory, or to view properties of a currently managed directory. This dialog also shows the URL to the LDAP server and the authentication information required to connect to the LDAP directory:

- **Directory URL:** Enables you to specify the LDAP directory to be managed. An example of an LDAP directory and the correct syntax is `ldap.<companyname>.com`. For example, you might type `ldap.xyzcompany.com`.
- **Authentication:** Enables you to log in as the following user (that is, you specify a user path and name and the user password).

About the Advanced LDAP query dialog

From the **Basic LDAP query** dialog, click **Advanced** to open the **Advanced LDAP query** dialog, which displays the following:

- **LDAP query root:** Enables you to select a root object in the directory for this query. The query that you're creating will return results from this point in the tree down.
- **LDAP query:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Examples:** Displays query examples you can use as a guide when creating your own query in freeform.
- **Test query:** Enables you execute a test of the query you have created.

The **Advanced LDAP query** dialog appears when you select to edit a query that has already been created. Also, if you select an LDAP group in directory manager and then choose to create a query from that point, the **Advanced LDAP query** dialog appears with a default query that returns the users who are members of that group. You can't change the syntax of this default query, only save the query.

More about the Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for accessing and viewing information about users and devices. LDAP enables you to organize and store this information into a directory. An LDAP directory is dynamic in that it can be updated as necessary, and it is distributed, protecting it from a single point of failure. Common LDAP directories include Novell Directory Services* (NDS) and Microsoft Active Directory Services* (ADS).

The following examples show LDAP queries that can be used to search the directory:

- Get all entries: (objectClass=*)
- Get entries containing 'bob' somewhere in the common name: (cn=*bob*)
- Get entries with a common name greater than or equal to 'bob': (cn>='bob')
- Get all users with an e-mail attribute: (&(objectClass=user)(email=*))
- Get all user entries with an e-mail attribute and a surname equal to 'smith': (&(sn=smith)(objectClass=user)(email=*))
- Get all user entries with a common name that starts with 'andy', 'steve', or 'margaret': (&(objectClass=User) (| (cn=andy*)(cn=steve*)(cn=margaret*)))
- Get all entries without an e-mail attribute: (!(email=*))

The formal definition of the search filter is as follows (from RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> | <or> | <not> | <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> | <filter> <filterlist>
- <item> ::= <simple> | <present> | <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> | <approx> | <ge> | <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL | <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL | <value> '*' <starval>
- <final> ::= NULL | <value>

The token <attr> is a string representing an AttributeType. The token <value> is a string representing an AttributeValue whose format is defined by the underlying directory service.

If a <value> must contain one of the characters * or (or), precede the character with the slash (\) escape character.

Managing inventory

LANDesk uses an inventory scanning utility to add devices to the core database and to collect device hardware and software data. You can view, print, and export inventory data. You can also use it to define queries, group devices together, and generate specialized reports.

Read this chapter to learn about:

Inventory

- Inventory scanning overview
- Viewing inventory data
- Tracking inventory changes
- Creating a custom data form

Note: For more information about running the inventory scanner, and inventory scanner troubleshooting tips, see [Additional inventory operations and troubleshooting](#).

Inventory scanning overview

The inventory scanner collects hardware and software data and enters it into the core database. When you configure a device with the Agent configuration tool, the inventory scanner is one of the components of the standard LANDesk agent that gets installed on the device. The inventory scanner runs automatically when the device is initially configured. A device is considered managed once it sends an inventory scan to the core database. The scanner executable is named LDISCN32.EXE and supports Macintosh, Linux, and Windows 95/98/NT/2000/2003/XP devices.

There are two types of inventory scans:

- **Hardware scan:** Hardware scans inventory hardware on managed devices. Hardware scans run quickly. You can configure the hardware scan interval in an agent configuration (**Tools | Configuration | Agent Configuration**) that you can deploy to managed devices. By default, hardware scans run each time the device boots.
- **Software scan:** Software scans inventory software on managed devices. These scans take longer to run than hardware scans. Software scans can take a few minutes to complete, depending on the number of files on the managed device. By default, the software scan runs once a day, regardless of how often the inventory scanner runs on the device. You can configure the software scan interval in the **Configure | Services | Inventory** tab.

You can scan a device on demand by finding it in the network view, and from its shortcut menu, and clicking **Inventory scan**.

Note: A device added to the core database using the discovery feature has not yet scanned its inventory data into the core database. You must run an inventory scan on each device for full inventory data to appear for that device.

You can view inventory data and use it to:

- Customize the network view columns to display specific inventory attributes
- Query the core database for devices with specific inventory attributes
- Group devices together to expedite management tasks, such as software distribution
- Generate specialized reports based on inventory attributes

You can also use inventory scans to keep track of hardware and software changes on devices, and generate alerts or log file entries when such changes occur. For more information, see *Tracking inventory changes* later in this chapter.

Read the sections below to learn more about how the inventory scanner works.

Delta scanning

After the initial full scan is run on a device, the inventory scanner only captures delta changes and sends them to the core database. By sending only changed data, network traffic and data processing times are minimized.

Forcing a full scan

If you want to force a full scan of the device's hardware and software data, use one of the following methods:

- Delete the INVDELTA.DAT file from the device. A copy of the latest inventory scan is stored locally as a hidden file named INVDELTA.DAT in each managed device's <LDMS_LOCAL_DIR>\Program Files\LANDesk\LDClient\Data folder.
- Add the **/sync** option to the inventory scanner utility's command line. To edit the command line, right-click the **Inventory scan** shortcut icon and select **Properties | Shortcut**, and then edit the **Target** path.
- On the core server, set the Do Delta registry key to 0, then stop and restart the LANDesk Inventory Server service. This key is located at:
HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Do Delta

Scan compression

Inventory scans performed by the Windows inventory scanner (LDISCN32.EXE) are compressed by default. The scanner compresses full scans and delta scans with approximately an 8:1 compression ratio. Scans are first built completely in memory, then compressed and sent to the core server. Scan compression requires fewer packets and reduces bandwidth usage.

You can disable inventory scan compression by setting the core server's Disable Compression registry key to 1. The default value, 0, enables compression. This key is located at:

HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Disable Encryption

Encrypted data transport

In **Configure | Services | Inventory** tab, there is an **Encrypted data transport** option. This option causes device scans to be sent to the core using SSL. Since the files are sent through the Web service and not the inventory service front end, a NAT address won't be appended to the scan file, even if that option is enabled in the registry.

Viewing inventory data

Once a device has been scanned by the inventory scanner, you can view its system information in the console.

Device inventories are stored in the core database, and include hardware, device driver, software, memory, and environment information. You can use the inventory to help manage and configure devices, and to quickly identify system problems.

You can view inventory data in the following ways:

- Viewing a summary inventory
- Viewing a full inventory

You can also view inventory data in reports that you generate. For more information, see Reports.

Viewing a summary inventory

Summary inventory is found on the device's properties page and provides a quick look at the device's basic OS configuration and system information. The summary also shows the date and time of the last inventory scan so you know how current the data is.

Note: If you added a device to the core database using the discovery tool, its inventory data isn't yet scanned into the core database. You must run an inventory scan on the device for the summary inventory feature to complete successfully.

To view summary inventory

1. In the console's network view, right-click a device.
2. Click **Properties | Inventory** tab.

Inventory summary data is different for Windows NT/2000/2003/XP and Windows 95/98 devices.

Viewing a full inventory

A full inventory provides a complete listing of a device's detailed hardware and software components. The listing contains objects and object attributes.

To view a full inventory

1. In the console's network view, right-click a **device**.
2. Click **Inventory**.

For detailed information, see About the Inventory window.

Viewing attribute properties

You can view attribute properties for a device's inventory objects from the inventory listing. Attribute properties tell you the characteristics and values for an inventory object. You can also create new custom attributes and edit user-defined attributes.

To view an attribute's properties, double-click the attribute.

For more information, see [About the Inventory attribute properties dialog](#).

Tracking inventory changes

LANDesk can detect and record changes about the device hardware and software. Tracking inventory changes can help you control your network assets. Inventory change settings let you select which types of changes you want to save and with what severity level. The selected changes can be saved in an inventory history log, the core server's Windows event log, or sent as an AMS alert.

You can view and print a device's history of inventory changes. Additionally, you can export the inventory changes to a .CSV formatted file for analysis using your own reporting tools.

To track and use inventory changes, you must first configure the inventory change settings. You will be able to perform the other inventory changes history tasks:

- Configuring inventory change settings
- Viewing, printing, and exporting an inventory changes

Configuring inventory change settings

Note: You must first configure these settings if you want to view, print, or export inventory changes for any devices on your network.

To configure inventory change settings

1. Click **Configure | Inventory history**.
2. In the **Inventory change settings** dialog, expand the **Computer** object in the **Current inventory** list, and select the system component you want to track.
3. In the **Log event in** list, select the component's attribute you want to track.
4. Check the appropriate box to specify where to record a change in that attribute. Inventory changes can be recorded in the inventory changes history log, Windows NT event viewer log, or as an AMS alert.
5. Select a severity level from the **Log/Alert severity** drop-down list. Severity levels include: None, Information, Warning, and Critical.
6. Click **OK**.

For more information, see About the Inventory change settings dialog.

Viewing, printing, or exporting inventory changes

To view, print, or export inventory changes

1. In the console's network view, right-click a device (or devices).
2. Click **Inventory history**.
3. Click **Print** to print the inventory changes history.
4. Click **Export** to save the inventory changes history as a .CSV file.

For more information, see About the Inventory changes history dialog.

Using custom data forms

LANDesk includes a custom data forms tool (**Tools | Custom data forms**) that you can use to create and manage forms. Custom data forms provide a way for you to collect information from users and add it to the core database.

Custom data forms are not supported in LANDesk Security Suite

Custom data forms is not available with a LANDesk Security Suite only license. You must have a full LANDesk Management Suite license in order to use the custom data forms feature.

The inventory scanner can't gather certain types of personalized user-specific information, such as:

- Where is a user's desk?
- What is a user's asset number?
- What is the user's phone number?

The best way to get this information is directly from your users with custom data forms.

Custom data forms have two main components: the form designer which is used by you to create forms for users to fill out, and the form viewer which is used by users to fill out forms.

Forms can be stored centrally or locally. If they're stored centrally, all users automatically have access to the latest forms because everyone views the same form from the same place. If forms are stored locally, you must ensure that users receive the latest forms.

After a user completes a form, the form viewer stores the results locally in C:\Program Files\LANDesk\LDCClient\LDCSTM.DAT. This file contains the results from all of the forms the user has responded to. If the user ever needs to fill out the same form again (for example, if the original form was revised), the form viewer fills in the form with the previously entered data.

The inventory scanner takes the information from each device's LDCSTM.DAT file and adds it to the core database.

Oracle databases are case-sensitive

When creating custom fields with custom data forms (or using any other feature) on an Oracle database, make sure you consistently capitalize field names. For example, data associated with "Cube location" is stored in a different place in the database than data associated with "Cube Location."

Also, make sure custom fields have names that are unique regardless of capitalization. The correct inventory data may not be retrieved if two custom fields have the same name but different capitalization.

For more information about custom data forms, see the following procedures:

- Creating a custom data form
- Creating a group of forms
- Configuring devices to receive custom data forms
- Filling out forms on the device

Creating a custom data form

Follow these steps to create a custom data form.

To create a custom data form

1. Click **Tools | Configuration | Custom data forms**.
2. In the Custom Data Forms window, double-click **Add new form**.
3. Enter a name for the form.
4. Enter a description for the form.
5. Click **Add** to open the **Add question** dialog.
6. In the Add Question dialog, type in the **Question text**, **Inventory name**, and **Description**.
7. Select the **Control type**.
8. Select whether you want the field to be required.
9. If you selected the **Edit** control type, click **Finish** to close the **Add question** dialog. The Edit control type lets users type in their own answers to questions in an editable text box. You can add more questions or proceed to step 12.
10. If you selected either of the **Combo box** control types, click **Next** to open the **Add items** dialog. The Combo box control type lets users select their answers from a drop-down list of pre-defined items.
11. In the Add Items dialog, enter an item name and click **Insert** to place the item in the Items list. These items appear in a drop-down list for that question on the form. You can add as many items as you like, then click **Finish**.
12. When you're done adding questions, click **Close** to save the form.

You can right-click on a form to schedule it for distribution to devices.

Creating a group of forms

If you have more than one form that you want to send to devices, you can organize them into a group. Then you can simply schedule the group of forms for distribution. Of course, this is not a required procedure.

When you schedule a group of forms for distribution, the local scheduler reads the contents of the group when it's time to distribute it. In other words, you can still change the contents of the group even after it has been scheduled (as long as the scheduled job hasn't yet occurred).

Note: If a form that is part of a group is later modified or deleted, the group automatically reflects those changes.

To create a group of forms

1. In the **Custom data forms** window, click the **Multiple forms toolbar button**.
2. Enter a name for the new group.
3. Select the forms you want to add to the group from the list of available forms.
4. Click **OK**.

You can right-click on a group of forms to schedule it for distribution to devices.

Configuring devices to receive custom data forms

When you set up devices, you can configure them to receive custom data forms. You must select to install the custom data forms component, and specify custom data form options on the agent configuration dialog. For more information, see [Deploying custom data forms](#).

In the agent configuration dialog, you need to specify how you want to update forms on the device:

- **Automatic update:** If all of the forms are stored centrally (automatic updates), users check a single location for new forms. That way, when a new form is available, all devices looking there have immediate access to it. The disadvantage is that users may see forms that aren't relevant to them.
- **Manual update:** If forms are stored locally (manual updates), you'll need to distribute the forms to the users that need to fill them out. There is less network overhead because each device has its own copy of the form. The benefit of local forms is that you can limit the forms users see to only those that are relevant to them. You copy forms to devices during device setup or with the Scheduled Tasks tool.

You also need to specify when forms will be shown on the device:

- **On startup:** The device's form viewer checks for any new or modified forms each time the device boots. The form viewer launches after the operating system loads. The next time the inventory scanner runs, it sends completed forms to the core database.
- **When the inventory scanner runs:** The inventory scanner starts the form viewer, which checks for any new or modified forms. As soon as users finish filling out the form and close the form viewer, the scan finishes and the data is entered in the core database.
- **Only in LANDesk program folder:** The form viewer can be launched manually from the LANDesk Management Suite program group. The next time the inventory scanner runs, it sends completed forms to the core database.

You can also use the **Scheduled tasks** window to launch the form viewer on devices at a predefined time. In this scenario, use the **Scheduled tasks** window to first distribute the forms to devices. Make sure to allow enough time to distribute the forms before you use the scheduled task scriptable jobs feature to run the form viewer.

Filling out forms on the device

When the form viewer launches on the device, a list of forms and each form's status displays:

- **New:** Indicates the form has never been filled out by this user.
- **Completed:** Indicates the user has opened this form and filled out, at a minimum, the required fields.
- **Do again:** Indicates the user has completed this form before, but the form has since changed. The user needs to look at the form again and make any necessary changes. Once this is done, the form's status changes to completed.

Once users select a form to fill out and click Open, a simple Form wizard appears. It contains a list of questions and fields for answers. If there are more questions than fit on a page, there are Back/Next buttons. Users can click Help (or press F1) while the cursor is in a field to display a help message generated by the **Description** field in the form designer.

Users must answer any required questions before continuing to the next page or exiting a form. Required questions have a red dot beside them.

The last page of the form wizard has a **Finish** button that users click when they're done. Clicking this button returns users to the **Form selection** dialog where the status message beside the form name is updated.

Using reports

The reporting tool can be used to generate a wide variety of specialized reports that provide critical information about the devices on your network.

Read this chapter to learn about:

- Reports overview
- Understanding reports and report groups
- Running and viewing reports
- Publishing reports
- Creating custom reports
- Using the report designer
- Importing and exporting reports
- Creating .CSV files

Reports overview

The reporting tool takes advantage of the robust inventory scanning utility, which collects and organizes hardware and software data, in order to produce useful, informative, and up-to-date reports (see Inventory scanning). You can use the standard (predefined) service and inventory reports, or create your own custom reports (see Creating custom reports). The predefined reports are provided by default with the application. The custom reports enable you to define a unique set of information with which to generate a report. The predefined or custom parameters are run and a report is generated containing the relevant data, which can be viewed from the console. Additionally, you can schedule reports to be published and saved to disk or to a secure file share location on your network where anyone with proper login credentials can access and view the reports. You can schedule the published reports to be e-mailed to designated recipients according to their rights and scope.

Understanding reports and report groups

Reports are organized in groups in the Reports window (**Tools | Reporting/Monitoring | Reports**). Administrators can view the contents of all of the report groups. Users with the Reports right can also see and run reports, as well as publish reports, but only on the devices included in their scope.

The left-hand pane of the **Reports** window shows a hierarchical view of the following report groups:

My reports

Lists the reports (and reports groups) you have added to your **My reports** group. These are typically reports that you run on a regular basis and have organized for your own use. They can be predefined or custom reports. Reports are run against the currently logged-in user's scope. An administrator has access to each user's reports groups and can add and remove reports (see User reports below).

All custom reports

Lists all of the custom reports on your core server, including those created or imported by yourself or another user. For more information, see Creating custom reports.

Standard reports

Lists the predefined reports that are provided with the application. The reports are preformatted, have query properties and chart types assigned, and are ready to be used.

Management Suite log files

Lists the log files for scheduled tasks that are run on your system. These log files provide status information about various services, tasks, actions, or events that are executed on devices on your network. The log files include delivery method statuses, multicast client and subnet representative statuses, OS deployment success rates, scheduled task statuses, and so on.

Note: Log files are typically stored in the \LANDesk\ManagementSuite\log directory. You can specify a different directory location during installation by changing the path.

Inventory reports

Lists all of the predefined inventory reports. Inventory reports provide information about devices on the network, including which devices are assigned to users, the software being run on devices, how devices are used, the type of hardware, memory utilization, load capacities, specifications, and so on.

Software licensing monitoring reports

Lists all of the predefined software license monitoring reports. The reports provide information about the type of software being used, the frequency of usage, volume rates, and denial instances in order to monitor usage and ensure compliance with software license agreements.

Note: Software License Monitoring reports are not constrained by the user's scope.

Remote control reports

Lists all of the predefined remote control reports. The reports maintain a history of remote control usage based on client, console, computer, duration, and so on.

Unmanaged devices reports

Lists all of the predefined unmanaged device discovery reports. The reports provide information about unmanaged devices, including device types, network locations, applied agents, and so on.

Security and Patch Manager reports

Lists all of the security and patch manager reports. The reports provide information about vulnerabilities, spyware, security threats, blocked applications, LANDesk updates, custom definitions, and so on. The reports can be produced based on device types, dates, locations, and other criteria.

User reports

Lists all reports for individual users, which are organized into subgroups by user. User subgroups are named with their login IDs, such as computername\user account or domain\user account. Each user group contains the reports that appear in that user's My Reports group.

As with the **User devices** and **User queries** groups, the **User reports** group can be seen ONLY by a user with the LANDesk Administrator right. Administrators can access a user's reports group to run reports against that user's scope, as if they were that user. In this way, an administrator can preview exactly what a user will see when they run a report.

Running and viewing reports

You run the reports from the **Reports** tool window by double-clicking the report, or right-clicking the report and selecting **Run**. If prompted, select the relevant report criteria, and then click **OK**. The report data displays in the report viewer (see Report viewer).

You can also run inventory reports directly from a device in the network view. From the network view, right-click the device you want to run a report for, click **Run inventory report**, and then double-click the report you want to run. If prompted, select the relevant report criteria, and then click **OK**. The report data displays in the **Report** viewer.

Note: Some reports are limited to a single device selection and will not run if more than one has been selected in the network view. A message box will notify you if the report cannot be run against multiple devices.

Report viewer

Once a report runs, the report viewer launches and displays the generated report with the specified information. This report viewer provides controls that enable you to display the report according to your viewing preferences. You can also export a report from the report viewer. The report viewer toolbar consist of the following:

- **Table of Contents:** Displays a table of contents for the report, if available. Click on a node in the tree to take you to that location within the report.
- **Print:** Opens your standard default printer dialog.
- **Copy:** Copies the contents of the report for the selected page.
- **Find:** Searches for a specific text string anywhere in the report data.
- **Single page view:** Displays the report as a single page.
- **Multiple page view:** Displays the report with multiple pages, which you can determine.
- **Zoom in:** Increases the size of the report.
- **Zoom out:** Decreases the size of the report.
- **Zoom percentage:** Selects the specific size of the report.
- **Previous page:** Takes you to the previous page in sequential order (compare with Backward).
- **Next page:** Takes you to the next page in sequential order (compare with Forward).
- **Page box:** Inserts a specific page number, which takes you directly to that page.
- **Backward:** Takes you to the previous page regardless of the numeric order.
- **Forward:** Takes you to the next page regardless of the numeric order.
- **Graph:** Determines whether to use a graph (none, bar, or pie), if available.
- **Sort:** Changes the sort order of the details of the report based on the selected column.
- **Export:** Enables you to export the report in HTML, PDF, XLS, DOC, and RTF formats.

Publishing reports

Publishing a report enables you to provide critical and timely information about your network devices to a controlled audience. When you publish a report, it is saved to a shared location on the network. The reports can be made accessible for viewing (see Sharing published reports), or sent to designated recipients (see E-mailing reports), even if they don't have access to the application. This enables the report to be shared with non-LANDesk users and reviewed at the reader's convenience. You can schedule reports to automatically be published at designated times, as well as configure them to reoccur on a regular basis (see Scheduling to publish a report).

Note: Reports don't have to be run before they are published. The report generation is performed during publishing. This can reduce bandwidth usage when you publish a large report that gathers and formats an extensive amount of data from across your network.

Defining a default user in the LANDesk reports user group

During the installation of LANDesk, you are prompted to create and define a user account in a user group called LANDesk Reports. This group controls access to the share where the published reports are stored. The default user group name is LANDesk Reports. You can change the name during installation. The LANDesk Reports user group shouldn't be changed after the application is installed.

You define a default user for this group by specifying a user name and password during installation. You can choose to clear this option during installation, but if you want to be able to provide access to published reports from a file share on a network, you should define the default user account. Send the default user's login information to the non-LANDesk users to give access to published reports. Existing LANDesk users can be added to the LANDesk Reports user group and use their own authentication, or be provided with the default user information as well. LANDesk users can be added to the LANDesk Reports group via the Windows NT users environment on the core server or by using local accounts (see Managing local accounts).

Publishing a report

When publishing a report, you can save the report file in any of the following formats: .HTML, .PDF, .XLS, .DOC, and .RTF.

To publish a report

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Locate the report you want to publish, right-click the report, and then click **Publish**.

Note: You do NOT have to run a report before publishing it.

3. If prompted, select the requested report criteria, and then click **OK**.
4. In the **Publish report** dialog, verify the name of the report (you can change this name if you like), verify the location where the report file is saved, specify the file format, and then click **Save**.

Note: The default storage location for published reports is in the **ldmain\reports** folder on your core server. This is the secured file share that only the LANDesk Reports user group has access to.

5. (Optional) In the **Report published** dialog, you can click **Preview** to verify the report's contents and formatting before sending the network path of the file share to recipients. You can also click **Copy path to clipboard** if you want to paste the full path and file name into another application for future reference, or directly into the body of an e-mail message to send to anyone you want to review the report.
6. Click **Close**.

Sharing published reports

Once a report is published to the shared folder on your core server, it can be accessed by an external audience if they have been given a valid user name and password to authenticate to the file share. Distribute the published report by sending your intended recipients the network path to the published report. The network path must contain the full path and filename. When the recipient accessed the file share, they are prompted to enter a valid user name and password for a user that is a member of the LANDesk Reports group before they can open and view the report. The default user for the LANDesk Reports user group is defined when you install the application (see Defining a default user in the LANDesk reports group). If you've added other users to the LANDesk Reports group, they can use their own user name and password to access the published report.

Scheduling to publish a report

Automating the publishing process ensures the scheduled report is made available promptly at the time you designate. With the report scheduling feature, you don't have to be physically present to initiate the publishing. Configuring the publishing of the report to reoccur on a regular basis free up valuable resources to perform other important tasks. This provides continual and reliable reporting. The ability to schedule when to publish a report is paramount to making critical information available at the required time.

Note: Scheduling a report to publish is limited to certain types of reports.

To schedule the publishing of a report

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click on the report you want to schedule to be published.
3. Select **Schedule Publish**. A task with the report name is created under **Scheduled Tasks** and is highlighted.
4. From the **Scheduled Tasks** tool, right-click on the task and select **Properties**.
5. Under **Schedule task**, enter the desired scheduling information.
6. Under **Recipients**, select where to deliver the report.
7. Click **Save**.

E-mailing reports

In order to e-mail a report, create a scheduled task of the report to be published and designate the intended recipients. The reports you configure to be e-mailed are automatically sent to the recipients every time a scheduled report is run. The content of the reports are based on the users scope. E-mailed reports are delivered in .PDF format. You have to provide an e-mail address for the intended recipients under their individual user properties (see Role-based administration help). Supplying an e-mail address will only make the users eligible to receive the report. You still need to select them as recipients from the scheduled task you create when you schedule the publishing of a report (see Scheduling to publish a report).

The following tasks must be completed before a report can be e-mailed to the intended recipients:

- Scheduling to publish a report
- Assigning e-mail addresses to users
- Selecting the recipients of a report
- Configuring SMTP for e-mailing reports

Assigning e-mail addresses to users

You must assign users e-mail addresses to make them eligible to receive reports. Once assigned, their user names will be available for selection as recipients when the schedule publishing task is created. For more information, see About the scheduled task - properties dialog.

To assign e-mail addresses to users

1. Click **Tools | Administration | Users**.
2. Right-click on the user and click **Properties**.
3. On the **User** tab, enter an e-mail address for the intended recipient of the report.
4. Click **OK**.

Selecting the recipients of a report

You can select the recipients of the report. The file share location on your core server is the default destination. Select the users you want to have the report e-mailed to. To add recipients to the list, see Assigning e-mail addresses to users. For more information, see About the scheduled task - properties dialog.

To select the recipients of a report

1. Click **Tools | Distribution | Scheduled tasks**.
2. Locate the scheduled task for the report you want to have e-mailed. Remember, the report must have been previously scheduled for publishing (see Scheduling to publish a report).
3. Right-click on the task of the report and select **Properties**.
4. Under **Recipients**, select the users you want to receive the report.
5. Click **Save**.

Configuring SMTP for e-mailing a report

Your outgoing mail server and the port number are required in order for reports to be e-mailed when a schedule publish task occurs. You can test your SMTP configuration to validate that it's set up correctly by sending a test e-mail to a designated address. For more information, see [About the scheduled task - properties dialog](#).

To configure SMTP for e-mailing a report

1. Click **Tools | Distribution | Scheduled tasks**.
2. Locate the scheduled task for the report you want to have e-mailed. Remember, the report must have been previously scheduled for publishing (see [Scheduling to publish a report](#)).
3. Right-click on the report and select **Properties**.
4. Under **SMTP configuration**, make sure the outgoing mail server (SMTP), the port number, the login information, and the test e-mail address are specified.
5. Click **Save**.

Creating custom reports

When creating custom reports, you specify what information will be displayed and how it will be displayed once the report is run. Each report consists of a query (custom or predefined), a layout (custom or predefined), and a graph selection (if applicable). The specified query will cause the appropriate data to be extracted from the database and populate the report at run time. The report is formatted according to the specified layout. The default report layout is used unless you choose otherwise. You can design a custom format using the report designer (see Using the report designer). For reports with graphing data, you can select a default grouping column and a graph type (pie, bar, or none) to have in the report.

Note: If you want a customer report with the same query data as a predefined report but in your own format, you will need to create a custom report that utilizes the same query parameters and then apply your formatting using the report designer.

You can create custom reports by right-clicking **My reports** from the Reports tool and then selecting **New custom report**. Administrators can also create custom reports by selecting a user from the **User reports** group by right-clicking a user and then selecting **New custom report**. Another method for creating custom reports is done directly from existing queries by right-clicking on a query and selecting **New custom report**. The New custom report icon can also be used to create a custom report. When you create a custom report, it's automatically added to the All Custom Reports group.

To create a custom report

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click on **My reports** and select **New custom report**.
3. From the **Reports properties** dialog, enter a title for the report, which also serves as the actual title of the report once it's generated.
4. Provide a description for the report, which also will be the formal description under the title in the final report.
5. Click **Select** or **Create** to specify a query.
6. If you want to alter the layout and formatting of the report, click **Design** to launch the report designer.
7. If applicable, choose the type of graph you want in your report.
8. Click **OK**.

Using the report designer

The report designer enables you to customize the layout and formatting of the reports you create in order to have the look and feel you require, whether it's to meet corporate style guides or produce a unique report. The layout and formatting capabilities of the report designer are similar to a desktop publishing application. You also have the additional functionality of having relational data fields within the report, which dynamically populate the report with data extracted from the database (see Data fields). The report designer is accessed from the Report Properties dialog when you create or modify a custom report (see Creating custom reports).

Note: Changing the title or description of the report from the report designer doesn't change the title and description in the **Report properties** dialog. You must change each one individually. Once you've made changes to the report layout, save the report and then make the corresponding changes in the dialog.

For information about the report designer, see the following sections:

- About the report designer
- Using report templates

About the report designer

Design Surface

The design surface acts as the canvas for the report. The report is segmented into specific content areas in a hierarchical order. The ReportHeader is always the top-tier node, and Details should always be the lowest-tier node. If you insert an additional GroupHeader (by right-clicking in the design surface), you may need to reorder the groups (also by right-clicking in the design surface). These report segments are collapsible and aid in the design process by keeping your surface area manageable. The grid, which can be turned on and off, is used to assist you with placing content on the design surface.

Toolbox

The toolbox consists of components (objects) that serve as the building blocks of the reports. They are placed onto the design surface in order to develop the structure and layout of your report. By inserting toolbox components, you begin to develop the foundation of your custom report. The toolbox is made up of the following components:

- **Pointer:** Selects components in the report. Just click a component on the design surface. Once a component is selected, you will be able to apply additional formatting, like resizing the component or applying different styles.
- **Label:** Inserts a label. Click and drag the box to define the boundaries of the label. The text of the label is added in the properties section while the label is selected.
- **Text box:** Inserts a textbox. Click and drag the box to define the boundaries of the text box. The text of the text box is added in the properties section while the text box is selected. Text boxes can be bound to a database field.
- **Checkbox:** Inserts a checkbox. Click and drag the box to define the width and height of the checkbox. Checkboxes can be bound to a database field.
- **Picture:** Inserts an image loaded from a file. Click and drag the box to define the width and height of the image. A dialog will prompt you to select an image for the picture component.
- **Shape:** Inserts a rectangle, circle, or square shape. Click and drag the shape to define its width and height.
- **Line:** Inserts a line. Click and then drag the line to the location you want the line to go.
- **Rich text box:** Inserts a rich text box. Click and drag the box to define the boundaries of the rich text box. When you release the button, a dialog will appear that enables you to select an RTF file. The content of the RTF file is placed in the rich text box. Clicking inside the rich text box will place a cursor in the box, which enables you to apply formatting to specific words. Rich text boxes can be bound to a database field.
- **Page break:** Inserts a page break.
- **Bar code:** Inserts a bar code. Click and drag the bar code to define the boundaries of the component. Bar codes can be bound to a database field.

Toolbars

The toolbars consist of standard formatting options, including text styles, fonts, font sizes, bold, italics, underline, justification, bullets, indentation, layering, and so on. Once the components have been placed onto the design surface, formatting can be applied to the components to achieve the desired appearance. Additional formatting is available from the Properties section. There are a few unique tools found on the toolbar:

- **OK:** Saves all changes and closes the report designer dialog.
- **Cancel:** Closes the report designer dialog without saving any changes.
- **New report:** Clears the report and provides a blank design surface in order to build a new report, however, you're still restricted to the same query fields you defined before entering the report designer.
- **Auto-generate report based on query:** Returns the report design to the original format before any changes were made. This enables you to restore the report to its original format according to the default settings.
- **Report settings:** Enables you to configure the report settings. The report settings consist of the following:
 - **Page Setup:** Defines the margins of the report.
 - **Printer Settings:** Defines the paper size, print orientation, and other print properties.
 - **Styles:** Enables you to create and edit font styles within the report
 - **Global Settings:** Provides grid controls and defines the unit of measurement.

Data fields

The data field values are aliases of the query parameters that you defined before opening the report designer. The data fields are proxies or placeholders that are linked to a data source. When you run the report, the data field is replaced with the information extracted from the data source. Initially, the data fields are automatically placed in the report. If you've deleted them or you're starting a new report, you can drag and drop the data fields back onto the design surface. You cannot create data fields from within the report designer. You must specify the data fields in the query before launching the designer (from the **Report query** dialog, click **Select Columns>>**).

Data fields should be used primarily in the Details section of the design surface, but can also be placed in a GroupHeader section. When you use data fields in the GroupHeader section, you must also apply a data field to the GroupHeader itself in order for it to propagate down and create instances for all the queried data. This is needed to properly group the data. For example, using a data field to serve as a heading, like "device name," insert the device name of every device in the database as the heading when the report is run. Each device name heading will be followed by the content designated in the details section (the next tier), which would be the rest of the data fields of the report. In the GroupHeader section of the design surface, the desired data field would be inserted first. Then the GroupHeader tag would be selected and have the data field in the Contents section changed to the same data field that was inserted into the data field.

Note: If you enter a data field value that doesn't exist according to the query, a missing data field box will appear above the data field box. Clicking the value provided in the missing data field box will select the erroneous data field on the design surface, so you will know which one to fix.

Contents

The Contents section contains a tree structure of the design surface. The main report is divided into the individual sections of the report. Any component placed onto the design surface in any given section is also represented in the tree under the corresponding report section. Clicking a node from the tree will select that item in the design surface, as well as display its properties directly underneath.

Properties

Each item, including report sections and components placed onto the design surface, has a unique set of properties. These properties are used to further configure your report and are more advanced than the standard formatting and layout tools. Not all properties are available for each node. Only the properties applicable to the selected item are given. The properties consist of the following:

- **Appearance:** Affects the look and feel of the selected item. All of the standard formatting tools are included.
- **Behavior:** Affects how the selected item will act.
- **Data:** Contains the actual content of the selected item, like textual information or a data field.
- **Design:** Provides a description of the selected item, which doesn't appear on the design surface.
- **Layout:** Provides the size and orientation of the selected item, like the location in terms of X and Y coordinates, or the size in terms of width and height.
- **Misc:** Contains any additional functionality for the selected item that is not included under the other property types.
- **Summary:** Enables you to create summations within the report. These total fields will automatically perform the mathematical equations at run time and display the computed value in the designated location.

Using report templates

You can create report templates to replace the default layout of a report. This makes it easier to create custom reports since a large portion of the customization will have already been performed. You only need to apply the report template to implement your custom look and feel. Once your template is loaded, you can further customize your new report as needed.

Note: Report templates only can be applied to custom reports.

Creating a report template

A report template is created from the report designer. You can alter the default template or another template and then save it as a template.

To create a report template

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click **My reports** and then click **New custom report**.
3. Provide a title, description, query, and chart type and click **Design**.

4. From the report designer, build your new template by making all design, layout, and format modifications.
5. Click **File | Save as Template**.
6. Provide a title and description and click **OK**.

Applying a report template

Once a template has been created, it can be applied to any custom report.

Note: Apply the template before making any changes to the report. Any changes made in the report before the template is applied will be lost. This cannot be undone.

To apply a report template

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click **My reports** and then click **New custom report**.
3. Provide a title, description, query, and chart type and click **Design**.
4. From the report designer, click **Tools | Templates**.
5. Select the template you want to apply and click **Load**.

Importing and exporting reports

The **Reports** tool supports both importing and exporting reports. You can transfer reports from one core database to another. The query is automatically imported and exported with the report since it is required by the report to display properly. Imported reports are placed into the **My reports**, **All custom reports**, and **User reports** groups.

Note: Changing the embedded query (XML) in the report will not produce a separate report. It will cause an error. If you want to make a change to the report, it must be done from the Reports tool in LDMS.

To import a report

1. Right-click the reports group where you want to place the imported report.
2. Select **Import** from the shortcut menu (or from the toolbar).
3. Navigate to the report file (.XML) you want to import and select it.
4. Click **Open** to add the report to the selected group in the network view.

You can export individual reports as well as entire reports groups and their contents.

To export a report

1. Right-click the report (or reports group) you want to export.
2. Select **Export** from the shortcut menu (or from the toolbar).
3. Navigate to the location where you want to save the report.
4. Type a name for the report.
5. Click **Save** to export the report.

Creating .CSV files

You can create comma-delimited files in plain text that are easily integrated into databases, spreadsheets, word processors, and so on. The file is created according to the inventory data that displays in the network view. These files are saved as generic .CSV files.

To create a .CSV file

1. Click **Tools | Reporting/Monitoring | Reports**.
2. Right-click **Reports** and select **New CSV report**.
3. In the **New .CSV report** dialog, enter a name for the report.
4. Select whether to report on all devices or only selected devices.
5. Select whether you will use the current column configuration in the network view, or if you will select a different column configuration.
6. Click **OK** to save the .CSV file with a name and directory location you specify.

Note: You can also export a .CSV asset report for use with other reporting tools. You can export a .CSV report in one of the following formats: HTML, RTF, or TXT.

Using scripts and tasks

LANDesk Management Suite includes a powerful scheduled task system. Both the core server and managed devices have services/agents that support scheduled tasks. Management Suite consoles and Web consoles can add tasks to the scheduler.

A task consists of:

- A distribution package, delivery method, targeted devices, and a scheduled time. Non-distribution tasks consist of a script, targeted devices, and scheduled time.

Here are some of the tasks you can schedule:

- Device configurations
- Various custom scripts
- Custom data form deployments
- Unmanaged device discoveries
- Vulnerability scans
- Software execution on managed devices

Completing the script creation dialogs for these tasks generates an ASCII text file in the Windows INI format with an .INI extension. These scripts are stored on the core server in the \Program Files\LANDesk\ManagementSuite\Scripts folder. The script filename becomes the script name in the console. Software distribution scripts are an exception. They don't create an INI file and are instead stored in the database. The scripts only contain information about the task being completed, not which devices the script will run on. The scripts use a custom scripting language unique to Management Suite. For more information on scripts, see "Processing custom scripts."

Read this chapter to learn about:

- Managing scripts
- Scheduling tasks
- Using the Scheduled tasks window
- Assigning targets to a task
- What you see when tasks run
- Monitoring task status
- Viewing task logs
- Using the default scripts
- Configuring local scheduler scripts

Managing scripts

LANDesk Management Suite uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (**Tools | Distribution | Manage scripts**) for these tasks:

- OS deployment/profile migration
- File transfer
- Custom scripts that you create
- Local scheduler scripts that run on a schedule you specify

The Manage scripts window divides scripts into three categories:

- **My scripts:** Scripts that you created.
- **All other scripts:** Scripts that shipped with Management Suite.
- **User scripts** (only visible to Management Suite administrators): Scripts created by all Management Suite users. These are sorted by the creator's username.

You can create groups under the **My scripts** item to further categorize your scripts. To create a new script, right-click the **My scripts** item or a group you've created and click the script type you want to create.

Once you've created a script, you can click Schedule on the script's shortcut menu. This launches the **Scheduled tasks** window (**Tools | Distribution | Scheduled tasks**) where you can specify devices the task should run on and when the task should run. See the next section for more information on scheduling tasks.

Due to specific capabilities supported by the Windows console, scripts created in the Windows console shouldn't be edited in the Web console.

Changes to script and task ownership for users of previous Management Suite versions

With Management Suite versions prior to 8.5, all scripts were global and all users could see them. In Management Suite 8.5, scripts are only visible to the script creator and Management Suite administrators.

The **Manage scripts** window (**Tools | Distribution | Manage scripts**) now has a **State** column. The **State** column shows **Public** if all users can see the script, or **Private** if only the user that created the script or administrators can see it. Users can right-click scripts they have created and toggle the **Public script** option on and off. Administrators can change the status of any script.

Scheduling tasks

The **Scheduled tasks** window shows scheduled task status and whether tasks completed successfully or not. The scheduler service has two ways of communicating with devices:

- Through the standard LANDesk agent (must already be installed on devices).
- Through a domain-level system account. The account you choose must have the log in as a service privilege. For more information on configuring the scheduler account, see "Configuring the scheduler service."

The console includes scripts that you can schedule to perform routine maintenance tasks such as running inventory scans on selected devices. You can schedule these scripts from **Tools | Distribution | Manage scripts | All other scripts**.

Using the Scheduled tasks window

Use the **Scheduled tasks** window to configure and schedule scripts you've created. Schedule items for single delivery, or schedule a recurring task, such as a script task to regularly search for unmanaged devices.

The **Scheduled tasks** window is divided into two halves. The left half shows task tree and tasks, and the right half shows information specific to what you've selected in the tree.

Left pane

The left pane shows these task groups:

- **My tasks:** Tasks that you have scheduled. Only you and Management Suite administrative users can see these tasks.
- **Common tasks:** Tasks that users have marked common. Anyone who schedules a task from this category will become the owner of that task. The task remains in the **Common tasks** folder and will also be visible in the **User tasks** group for that user.
- **All tasks:** Both your tasks and tasks marked common.
- **User tasks** (Management Suite administrative users only): All tasks users have created.
- **All policies:** Any task that is active as a policy. These tasks also appear in the other task groups. This group provides a convenient way of seeing active policies.

You can drag scripts onto the **Scheduled tasks** window's left pane. Once a script is in the left pane, you can configure targets for it by dragging devices, queries, or groups to the right pane.

When you click **My tasks**, **Common tasks**, or **All tasks**, the right pane shows this information:

- **Task:** The task names.
- **Start On:** When the task is scheduled to run. Double-click a task name to edit the start time or to reschedule it.
- **Status:** The overall task status. View the right pane **Status** and **Result** columns for more details.
- **Owner:** The name of the person who originally created the script this task is using.

When you click a scheduled task, the right pane shows this summary information:

- **Name:** The task state name.
- **Quantity:** The number of devices in each task state.
- **Percentage:** The percentage of devices in each task state.

When you click a task status category under a task, the right pane shows this information:

- **Name:** The device name.
- **Status:** The task status on that device (for example, "Waiting").
- **Result:** Whether the task ran successfully on the device.
- **LDAP object name:** If the device was targeted through LDAP, the LDAP object name.
- **Query name:** If the device was targeted through a query, the query name.
- **Message:** Custom messages from the device. These are used with tasks that run a DOS batch file. Include a command that launches sdclient.exe with a /msg="<Message you want to send>" command-line parameter.
- **Log file:** If a device failed to complete the task, the path to the task log file for that device is here.

Before you can schedule tasks for a device, it must have the standard LANDesk agent and be in the inventory database.

To schedule a task

1. In the **Manage scripts** window, click **Scripts | My scripts** or **All other scripts**, and the script you want to distribute.
2. Click the **Schedule** button. This displays the **Scheduled tasks** window and adds the script to it, where it becomes a task.
3. In the **Network view**, select the devices you want to be task targets and drag them onto the task in the **Scheduled tasks** window.
4. In the **Scheduled tasks** window, click **Properties** from the task's shortcut menu.
5. On the **Schedule task** page, set the task start time and click **Save**.

You can add more devices to the task by dragging them from the network view and dropping them on the task you want in the **Scheduled tasks** window.

Canceling a task

You can cancel waiting or active tasks. The way to cancel a task depends on the task type, as described below.

- **Software distribution tasks:** Use the cancel button on the toolbar. This toolbar button is only available for software distribution tasks.
- **Custom scripts:** From the shortcut menu of the script you want to cancel, click **Current status**. The **Task status** dialog has **Discontinue task** and **Cancel task** buttons. Click the button you want.
- **Waiting tasks:** From the shortcut menu of the task you want to cancel, click **Properties**. On the **Schedule task** page, click **Leave unscheduled**.

Understanding the Common tasks folder

The **Common tasks** group provides a convenient way for multiple users to access the same task. Tasks marked common appear in the **Common tasks** group as well as in the **User tasks** group for the user that last modified the task. Having the task in both places allows multiple users who share similar responsibilities to access and modify the task.

A user can mark any task that is visible to them as common. Once a user clears the common option, the task is only visible in their **User tasks** group.

To mark a task common

1. From the shortcut menu of the task you want to make common, click **Properties**.
2. On the **Overview** tab, check **Show in common tasks**.

Assigning targets to a task

Once you've added a script to the **Scheduled tasks** window, you can assign targets to it. Drag targets from the network view onto the task that you want in the **Scheduled tasks** window. Targets can include individual devices, device groups, LDAP objects, LDAP queries, and inventory queries. Queries and groups are powerful options that let you have a dynamic list of devices that can change for recurring tasks. For example, as the device target list from a query changes, any tasks using that query will automatically target the new devices.

If a device is targeted more than once, such as when two target queries have overlapping results, the core server detects the duplication and won't run the task multiple times for the same device.

When using queries for task targets, the query won't run until the task is started. The **Scheduled task properties** dialog won't show the target devices until after the task is launched.

Applying scope to tasks

For scheduled tasks, multiple Management Suite users can add targets to a task. However, in the **Scheduled tasks** window, each Management Suite user will only see targets within their scope. If two Management Suite users with scopes that don't overlap each add 20 targets to a task, each Management Suite user will see only the 20 targets they added, but the task will run on all 40 targets.

Selecting targets for your task

Each task you create needs a set of targets that the task will run on. Tasks can have two types of targets, static and dynamic.

- **Static targets:** A list of specific devices or users that doesn't change unless you manually change it. Static targets can be LDAP users or devices from Directory Manager or devices from the console's network view.
- **Dynamic targets:** A dynamic list of devices that allows policy-based distribution tasks to periodically check the target list for any changes. Dynamic targets include query results and LDAP groups/containers or network view groups.

Dynamic policy targets are unique, in that Management Suite updates the results of these queries periodically. As new devices meet the query criteria, recurring tasks using those queries get applied to the new devices.

You can specify static policy targets in these ways:

- **Network view devices:** A static set of devices from the core database.
- **LDAP users or devices:** A static set of user and/or device objects.

You can specify dynamic policy targets in these ways:

- **Network view group:** A dynamic set of devices from the core database.
- **LDAP group/container:** A dynamic set of user and/or device objects.
- **Database query:** A set of devices generated by a query against the core database.
- **User group:** A group of users selected from an LDAP-compliant directory.
- **LDAP query:** A set of users, devices, or both, generated by a query on an LDAP-compliant directory.

Targeting devices through a directory

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct device software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager.

Windows 95/98 devices need to be configured to log into the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require policy-based management. As of this printing, more information on installing Active Directory device support was available here:

<http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utls/dsclient.msp>

For each Windows NT/2000/2003/XP device, there must be a computer account on the Active Directory domain controller. This means that the computer being used as the device must be logged into the domain where the Active Directory exists. You can't simply map a network drive using the fully-qualified Windows NT domain name. The policy won't take effect this way.

To use Directory Manager to create a query

1. Click **Tools | Distribution | Directory manager**.
2. Click the **Manage directory** toolbar button.
3. Enter the directory URL and authentication information and click **OK**.
4. Click the **New query** toolbar icon.
5. Create your query. For more information, see "Using LDAP queries."

What you see when tasks run

The **Scheduled tasks** window always shows job status. If you're scheduling device configurations or OS deployments, you'll also see the **Client setup utility** dialog. As the scheduler service proceeds through the target list, you'll see the devices to be configured, devices being configured, and devices completed lists. For more information, see "About the Client Setup Utility dialog."

If you're scheduling Targeted Multicast distributions, you'll see the **Multicast software distribution status** window. This window shows multicast status. For more information, see "About the Multicast Software Distribution Status window."

If you're scheduling custom scripts, you'll see the **Custom job processing** window showing scheduled, working, and completed targeted devices, in addition to a line-by-line script status as it executes.

Monitoring task status

When a task starts processing, targeted devices move through various task states. You can monitor the task state for targeted devices by clicking an active task in the Scheduled tasks window. Devices will be in one of these categories:

- **All devices:** All targets for the task.
- **Active:** Targets that are currently being processed.
- **Pending:** Targets that haven't been processed yet.
- **Successful:** Targets that completed the task successfully.
- **Failed:** Targets that failed the task.

These are the states the device can be in, and the category they are visible in:

- **Waiting:** Ready to process a task. (**Pending** category)
- **Active:** Processing the current task. (**Active** category)
- **Done:** Task processed successfully. (**Successful** category)
- **Busy:** Device is already processing a different task and couldn't process the current task. (**Failed** category)
- **Failed:** Didn't complete processing the task for some reason. (**Failed** category)
- **Off:** Device was off or unreachable. (**Failed** category)
- **Canceled:** The user cancelled the task. (**Failed** category)

Viewing task logs

If a device fails to process a task, the **Scheduled tasks** window stores the task log. Available logs appear in the **Log file** column next to a device. In the log file you can see the task command that failed.

Using the default scripts

Management Suite ships with a default set of scripts that are listed below. You can use them to help you complete some Management Suite tasks. These scripts are available under the **All other scripts** tree in the **Manage scripts** window (**Tools | Distribution | Manage scripts**):

- **am_verifyall:** Verifies all packages installed via policies on clients
- **Generic sample dir command:** Uses an OS deployment script to demonstrate rebooting a device with a virtual disk and running a dir command.
- **inventoryscanner:** Runs the inventory scanner on the selected devices.
- **multicast_domain_discovery:** Does a Targeted Multicast domain representative discovery. For more information, see "Using Targeted Multicast with Software Distribution."
- **multicast_info:** Runs a troubleshooting script that shows what information the Scheduled Tasks window will pass to Targeted Multicast, including target device IP addresses and subnet information. Creates a file called C:\MCINFO.TXT.
- **MSI service deployment:** Deploys the MSI service required for a PXE representative.
- **PXE representative deployment:** Deploys or updates a PXE representative.
- **PXE representative removal:** Removes the PXE service software from a PXE representative.
- **Restore client records:** Runs the inventory scanner on selected devices, but the scanner reports to the core the device was configured from. If you have to reset the database, this task helps you add devices back to the proper core database in a multi-core environment.
- **Uninstall metering client:** Removes the software metering agent on target devices. This agent was used in Management Suite prior to version 8.

Configuring local scheduler scripts

The local scheduler is a service that runs on devices. It's part of the common base agent and you can install it through device setup. Usually the local scheduler handles Management Suite tasks, such as running the inventory scanner periodically. Other tasks that you schedule, such as software or OS deployments, are handled by the core server rather than the local scheduler. You can use the local scheduler to schedule your own tasks to run periodically on devices. Once you create a local scheduler script, you can deploy it to devices by using the **Scheduled tasks** window.

The local scheduler assigns each task an ID number. Local scheduler scripts have an ID range that is different from the default local scheduler scripts that Management Suite uses. By default, you can only have one custom scheduler script active on each device. If you create a new script and deploy it to devices, it will replace the old script (any script in the custom local scheduler ID range) without affecting the default local scheduler scripts, such as the local inventory scan schedule.

When selecting schedule options, don't be so restrictive that the task criteria are infrequently met, unless that's your intention. For example, while configuring a task, if you select Monday as the day of the week and 17 as the day of the month, the task will only execute on a Monday that's also the 17th of the month, which happens very infrequently.

To configure a local scheduler command

1. In the **Managed scripts** window (**Tools | Distribution | Managed Scripts**), from the My scripts shortcut menu, click **New local scheduler script**.
2. Enter a **Script name**.
3. Click **Add** to define the script options.
4. Configure the local scheduler options as described earlier.
5. Click **Save** to save your script.
6. Use the **Scheduled tasks** window to deploy the script you created to devices.

Understanding bandwidth options

When configuring local scheduler commands, you can specify the minimum bandwidth criteria necessary for the task to execute. The bandwidth test consists of network traffic to the device you specify. When the time comes for the task to execute, each device running the local scheduler task will send a small amount of ICMP network traffic to the device you specify and evaluate the transfer performance. If the test target device isn't available, the task won't execute.

You can select these bandwidth options:

- **RAS:** The task executes if the device's network connection to the target device is at least RAS or dialup speed, as detected through the networking API. Selecting this option generally means the task will always run if the device has a network connection of any sort.
- **WAN:** The task executes if the device's connection to the target device is at least WAN speed. WAN speed is defined as a non-RAS connection that's slower than the LAN threshold.
- **LAN:** The task executes when the device's connection to the target device exceeds the LAN speed setting. LAN speed is defined as anything greater than 262,144 bps by default. You can set the LAN threshold in agent configuration (**Tools | Configuration | Agent | Configuration, Bandwidth detection** page). Changes won't take effect until you deploy the updated configuration to devices.

Using remote control

Use LANDesk Management Suite's remote control feature to easily resolve device problems from one location. You can only remote control devices that have the remote control agent installed. During a remote control session, the remote device actually has two users—you and the end user. You can do anything at the remote device that the user sitting at it can do. All of your actions are in realtime on that device.

Management Suite enables you to remote control these device types:

- Windows NT/2000/2003/XP devices
- Windows 95/98 devices
- NetWare servers
- Mac OS 9.2, 10.2.x, 10.3.x, and 10.4.x devices

Read this chapter to learn about:

- Using the remote control viewer
- Connecting to devices
- Remote controlling devices
- Using the drawing tools on remote devices
- Adjusting remote control settings
- Chatting with remote devices
- Transferring files to remote devices
- Running programs on remote devices
- Rebooting remote devices
- Changing device remote control security
- Using remote control logging
- Customizing the viewer and remote control agents

Using the remote control viewer

Use the remote control viewer to remotely access a device. You can only remote control devices that have the remote control agent installed. During a remote control session, the remote device actually has two users--you and the end user. You can do anything at the remote device that the user sitting at it can do.

You can do a lot more than just remote control a device from the viewer window. Once the viewer connects to a device, you can choose from these tasks:

- Remote control: Remotely view and control a device.
- Chat: Remotely chat with a device.
- File transfer: Remotely transfer files to and from your computer to another device. In essence, this works as though you've mapped a drive to remote device.
- Reboot: Remotely reboot a device.
- Draw: Displays drawing tools you can use to draw on the remote screen.

You can do multiple viewer tasks on a device at the same time. When you activate a viewer task, the interface for that task appears in the viewer window.

Once you've taken control of a remote device, its screen appears in the viewer window. Because the viewer window often isn't as big as the remote device's screen, you'll either need to use the autoscroll feature to scroll up, down, and side to side, or use the **Move Remote Screen** icon to maneuver more easily around the different areas of the remote screen. Also, autoscroll automatically scrolls the window as the mouse pointer approaches the viewer window's edge.

You can also increase the viewer window displayable area by disabling items in the View menu, such as connection messages, the toolbar, or the status bar. Use the **View** menu's **Full screen** option to completely remove the viewer window's controls. If the remote screen's resolution exceeds yours, autoscroll will still be necessary.

If you want to speed up the viewing rate or change the viewer window settings, use the items under the **Options** menu. To remotely chat, transfer files, or reboot the device, use the items under the **Tools** menu or the toolbar.

Connecting to devices

Before you can do any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see connection messages and status in the **Connection messages** pane, if that is visible. If it isn't, you can toggle it by clicking **View | Connection messages**.

To connect to a device

1. In the network view, from the shortcut menu for the device you want to remote control, click **Remote control, Chat, File transfer, or remote execute**.
2. Once viewer window appears and connects to the remote device, you can use any of the remote control tools available from the viewer's **Tools** menu, such as chat, file transfer, reboot, inventory, or remote control.
3. To end a remote control session, click **File | Stop connection**.

Remote controlling devices

Once you've connected to a device, often you'll want to view it remotely.

To view a remote device

- Click **Tools | Remote control**. If options in the **Tools** menu are dimmed, that means you aren't connected to a device.

To view different areas of a remote device screen

1. Move the mouse pointer to the edge of the viewer window. The window scrolls automatically.

OR

1. Click the **View another part of the remote screen** icon.
2. Your cursor becomes a hand that you can click, drag, and release to view various areas of the remote screen.

Using the drawing tools on remote devices

Once you're remotely viewing a device, you can use the drawing tools on it. The drawing tools can help you explain to users what you're doing or highlight information on the remote screen for users to look at. When you use a tool to draw on the screen, both you and the remote user can see what you've drawn. The drawn images stay on both your screens until you click the eraser in the drawing tool palette.

You have three drawing tools to choose from:

- **Pencil:** Use the pencil tool to make freehand drawings. You aren't limited to a shape with the pencil tool.
- **Box:** Use the box tool to draw a rectangle around something on the screen. Click where you want a corner of the rectangle to be, and while holding down the mouse button, drag it over the area you want boxed. Release the mouse button when you're ready for the rectangle to be drawn.
- **Pointer:** Use the pointer tool to point at objects on screen. When you hold down the left mouse button, the pointer tool is active and a red dot appears under the mouse pointer that makes it easy for users to see where the pointer is. When you release the left mouse button, the dot disappears. You can't change the dot color and it doesn't leave a trail like the pencil tool does.

You can also use the line thickness and line color drop-down lists to change how your drawings will look. Changes to these items only affect new things that you draw.

When you're done drawing, click the eraser button on the drawing palette or close the palette.

Adjusting remote control settings

Use the **Options** dialog's **Change Settings** tab (**Tools | Options**) to adjust the remote control settings.

- **Allow autoscroll:** Enables the viewer window to scroll as you move the cursor closer to the window border. The closer you move to the border, the faster the scrolling occurs.
- **Lock out the remote keyboard and mouse:** Locks the remote device's keyboard and mouse so that only the user running the viewer can control the remote device. Note that special key combinations in Windows such as "CTRL-ALT-DEL" or the "Windows Key+L" aren't locked out.
- **Synchronize clipboards to paste between local and remote computers:** Synchronizes the keyboards between the local and remote device so you can paste information between the two devices.
- **Blank the remote computer screen:** Blanks the remote device's screen so only the user running the viewer can see the user interface display on the remote device.
- **Lock the remote computer when the session ends:** When the session ends, activates the operating system's lock feature.

Optimizing remote control performance

Use the **Options** dialog's **Optimize performance** tab (**Tools | Options**) to optimize remote control performance for these connection types:

- Slow connection (modem)
- Medium connection (broadband)
- Optimize for fast connection (LAN)
- Custom connection

Changing the optimization setting dynamically adjusts color reduction, wallpaper visibility, and remote windows appearance effects (the ones you can adjust in **Display Properties | Appearance | Effects**), such as transition effects for menus and tooltips.

Remote control always uses a highly efficient compression algorithm for remote control data. However, even with compression, it requires a lot of data to send high color depth information. You can substantially reduce the amount of remote control data required by reducing the color depth displayed in the remote control viewer. When the viewer reduces the color depth, the viewer has to map the full color palette from the remote desktop to a reduced color palette in the viewer. As a result, you may notice colors in the remote control window that don't accurately reflect the remote desktop. If that's a problem, select a higher-quality compression setting.

Another way you can optimize performance is to suppress the remote wallpaper. When you do this, remote control doesn't have to send wallpaper updates as parts of the remote desktop are uncovered. Wallpaper often includes bandwidth-intensive images, such as photographs. These don't compress well and take time to transfer over slower connections.

The final way you can optimize performance is to use a mirror driver on the remote device. For more information, see the next section.

Using the mirror driver

The mirror driver provides many benefits. The main benefit is that it provides a Microsoft-supported way of capturing screen output without requiring modifications to the existing video driver. This allows the remote control mirror driver to behave in a standard way that can cause fewer problems on devices.

The other benefit is that the mirror driver doesn't use as much processing power from the target device. If you're remote controlling devices that have a 1.5 GHz or slower processor, the mirror driver can provide noticeable performance improvements over faster network connections. On slower network connections, remote control performance is limited more by bandwidth than processor utilization.

The standard remote control agent is always installed on devices. When the mirror driver is installed with it, the standard agent and the mirror driver coexist. You can't uninstall the standard remote control driver and use only the mirror driver.

Chatting with remote devices

You can use the remote control viewer to remotely chat with a user at a remote device. This feature is useful if you need to give instructions to a remote user whose dial-up connection is using the only available phone line. Users can respond back using the chat window that appears on their screen. You can only use chat on devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

If you want to save the messages from a chat session, you can. Any text appearing in the gray area of the chat session will be saved to a text file.

To chat with a user at a remote device

1. Click **Tools | Chat**. A section of the viewer window turns into a chat area.
2. In the lower left section of the chat area, type in a short message. Click **Send**.

Your message will appear on the remote device's screen. A user can respond by typing a message and clicking **Send**. The user also can click **Close** to exit out of a chat session.

To save messages from a chat session

1. In the chat area of the viewer window, click **Save messages**.
2. In the **Save as** dialog, type in a filename and click **Save**.

Transferring files to remote devices

You can use the remote control viewer to transfer files to and from your computer to the remote device. In essence, this works as though you've mapped a drive to the remote device. You can only transfer files to/from devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

To transfer files to a device

1. Click **Tools | File Transfer**. Windows Explorer appears.
2. Select a file to transfer by clicking the filename. From the file's shortcut menu, click **Copy**.
3. Scroll down the Windows Explorer tree to **LANDesk Remote Control**. You should see the name of the remote device you're currently controlling.
4. On the remote device, select a folder to paste the file to, then right-click and click **Paste**.

Similarly, you can also transfer files from a remote device to your computer.

Running programs on remote devices

You can launch programs on remote devices. Use the Run box on the viewer toolbar to enter the remote program's path and filename. Since the program will be launched on the remote device, the path and filename you enter must be present on the remote device.

To run a program on a remote device

1. In the viewer's **Run** box, enter the program path and filename. If you don't know either, you can drop down the list and click **Browse**. This opens a dialog that allows you to browse the remote device's folders.
2. Click the Remote execute button to the right of the **Run** box.

Rebooting remote devices

You can use the remote control viewer to remotely reboot a device. You can only remotely reboot devices that have the remote control agent installed. This feature works even if you're not viewing a remote device's screen.

To remotely reboot a device

1. Click **Tools | Reboot**.
2. In the **Timeout (seconds)** edit box, enter the time that a user will have before the device is rebooted. The maximum delay is 300 seconds.
3. In the **Remote user prompt** box, type in a brief warning message that a user will see on the device before it's remotely rebooted.
4. You can save your settings by clicking **Save these settings**.
5. Click **OK**.

The warning message will appear on the device, with a countdown showing how much time remains before the reboot. The user has the option of clicking **OK** to immediately reboot, or **Cancel** to not accept the request. A message box will appear on your computer telling you if the user cancelled the request. If the reboot has taken place, you'll see a message in the session messages area of the viewer window.

Changing device remote control security

Management Suite has a high level of control over devices when granted access rights. The device controls remote access security. It stores its remote access security settings in the registry.

You can change remote control settings and security model on clients by updating the agent configuration settings (**Tools | Agent configuration**), and from the updated configuration's shortcut menu, clicking **Schedule update**. Once you deploy the update to devices, their agents will use the settings you specified.

For more information, see "Deploying remote control."

Using remote control logging

By default, Management Suite logs remote control actions, including the device remote controlled and the console doing the remote controlling. You can disable remote control logging if you want or purge remote control log entries older than a date you specify. If logging is enabled, you can view these remote control reports (**Tools | Reporting/Monitoring | Reports**, and in the **Reports** tool, click **Reports | Standard reports | Remote control**):

- Remote Control History by Client
- Remote Control History by Console
- Remote Control History for Managed Computer
- Remote Control Summary

To enable or disable remote control logging

1. Click **Configure | Remote control logging**.
2. Check or clear the **Enable remote control logging** option, depending on your preference.

To purge the remote control log

1. Click **Configure | Remote control logging**.
2. Enter the date you want purged. All entries older than this date will be deleted.
3. Click **Purge Now** to execute the purge.

Customizing the viewer and remote control agents

The remote control viewer has command-line options you can use to customize how it works. You can also adjust the remote control agent registry keys on devices if necessary. Normally these registry keys are set by the remote control agent configuration that you deploy to devices.

Viewer command-line options

You can launch the remote control viewer using a command-line option that immediately opens a viewer window, connects to a specific device, and activates the viewer features you want, such as remote control, chat, file transfer, or device reboot.

Remote control command-line options use the following syntax:

```
isscntr /a<address> /c<command> /l /s<core server>
```

Option	Description
/a<address>	Contact a device at a particular TCP/IP address. The TCP/IP address may include both numeric- and name-style addresses, separated by semicolons. You can also specify the hostname.
/c<command>	<p>Start the remote control viewer and run a particular feature. (See command names below.) You can specify multiple /c arguments on one command line. For example:</p> <pre>isscntr /agamma /c"remote control" /c"file transfer"</pre> <p>You can choose from these features:</p> <p>Remote control: Open a remote control window</p> <p>Reboot: Reboot the given device</p> <p>Chat: Open a chat window</p> <p>File transfer: Open a file transfer session</p> <p>System info: Opens a window displaying information about the device, including OS, memory, and hard drive space.</p>
/l	Limit the viewer interface so it only displays the features you specify with /c.
/s<core server>	If you're using certificate-based security, use this option to specify the core server to authenticate with. This option is helpful if you're remote-controlling clients in a multi-core environment.

Example 1

Opens the viewer window. Any changes made, such as sizing the connection messages window or setting performance options are retained from the last time the viewer window was used.

```
isscntr
```

Example 2

Launches a remote control session connecting to the device named "gamma." (Note that there is no space and no punctuation between "/a" and "gamma.")

```
isscntr /agamma /c"remote control"
```

Example 3

Launches a remote control and chat session connecting to the device named "gamma." Remote control first attempts to try to resolve the name "gamma." If this fails, it attempts to connect to the numeric address 10.10.10.10:

```
isscntr /agamma;10.10.10.10 /c"remote control" /c"chat"
```

Port 9535 is used to communicate between the viewer and agent computers. If devices running issuser.exe are configured to use a port other than 9535, the port must be passed as part of the address given to isscntr.exe. For example, to remote control a device with address 10.4.11.44, where issuser.exe is configured to use port 1792 as the verify port, the command line would be:

```
isscntr /a10.4.11.44:1792 /c"remote control"
```

Macintosh agents still use ports 1761 and 1762 to communicate, but you can still use isscntr.exe in Management Suite 8.6 to remote control.

The NetWare agent uses port 1761.

Agent registry keys

You can modify the following registry settings on devices running the remote control agent.

The following registry keys are located under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\WUSER32
```

Key	Type	Purpose
Allow Chat	DWORD	Indicates if chat is allowed. Specify 1 to allow chat (the default) or 0 to block.
Allow File Transfer	DWORD	Indicates if file transfer is allowed. Specify 1 to allow file transfer (the default) or 0 to block.
Allow Takeover	DWORD	Indicates if takeover is allowed. Specify 1 to allow takeover (the default) or 0 to block.
Allow Remote Execute	DWORD	Indicates if remote execute is allowed. Specify 1 to allow remote execute (the default) or 0 to block.
Allow Reboot	DWORD	Indicates if remote reboot is allowed. Specify 1 to allow remote reboot (the default) or 0 to block.
Permission Required	DWORD	Indicates if the remote user is notified when the user running the remote control viewer attempts to connect to the device. Specify 0 (the default) to allow the viewer to take control without notification. Specify 1 to have a dialog pop up asking "Will you allow <the remote control viewer> to <remote control function> your machine?"
Single Permission	DWORD	When permission is required, this option controls whether permission is asked for each remote control feature (chat, file transfer, and so on) or whether a single

		acknowledgement allows all remote control features for that session. Specify 1 for permission to last the whole session, or 0 to prompt for each remote control feature.
System Tray Visible Signal	DWORD	The remote control icon in the system tray changes to indicate when the device is being remote controlled. Specify 1 to enable or 0 to disable.
System Tray Always Visible	DWORD	The remote control icon in the system tray is always visible. Specify 1 to enable or 0 to disable.
Visible Signal	DWORD	A remote control icon appears on the desktop when the device is being remote controlled. Specify 1 to enable or 0 to disable.

Troubleshooting remote control sessions

This section describes problems you may encounter when remote controlling a device and possible solutions.

I can't remote control a device

Check that the device has the LANDesk agents loaded.

To check that the LANDesk agents are loaded:

- In the console's network view, click **Properties** from the device's shortcut menu. Click the **Agents** tab and view the loaded agents.

To load the remote control agent

- Create an agent configuration task in the console and push it to the device, or map a drive from the device to the core server and run the appropriate device configuration task.

Can't transfer files between the console and a target device

Check to see if you're running Norton AntiVirus*, and if its Integrity Shield is turned on. If the Integrity Shield is turned on, you must have temporary privileges that let you copy to the directory that the Integrity Shield is protecting.

Using software distribution

This chapter explains how to use LANDesk Management Suite to distribute software and files to devices throughout your network.

Read this chapter to learn about:

- Software distribution overview
- Understanding package types
- Understanding the available delivery methods
- Setting up the delivery server
- Configuring Windows 2003 Web servers for software distribution
- Distributing a package
- Working with distribution owners and rights
- About file downloading
- Updating package hashes
- Using Targeted Multicast with software distribution
- About byte-level checkpoint restart and dynamic bandwidth throttling
- Distributing software to Linux devices
- Troubleshooting distribution failures

Software distribution overview

Software distribution enables you to deploy software and file packages to devices running the following operating systems:

- Windows 95B/98SE
- Windows NT (4.0 SP6a and higher)
- Windows 2000/2003/XP
- Mac OS X 10.2.x. and 10.3.x
- Linux RedHat 3.0 (AS, ES and WS)
- Linux Suse 9.1

Devices receiving the software distribution packages must have the following LANDesk agents installed:

- Standard LANDesk agent (formerly known as CBA)
- Software distribution agent

Software distribution features include:

- LANDesk Targeted Multicasting™ features that minimize bandwidth use when distributing large packages to many users—without dedicated hardware or router reconfigurations
- Delivery methods enable detailed control over how tasks complete
- Easy task scheduler integrates with the inventory database to make target selection easy
- Real-time status reporting for each deployment task
- Policy-based distributions, including support for create push tasks supported by policy
- Distribution to Mac OS 9.22 and Mac OS X devices
- Mobile device support, including bandwidth detection, checkpoint restart, and the ability to complete the job using a policy
- Full-featured package builder
- Ability to distribute any package type, including MSI, setup.exe, and other installers

If you don't have an existing package that you want to deploy, you can use Management Suite's package-building technology to create a standalone executable program for the required software installation. Once you have a package, store it on a Web or network server called a "delivery server." Through the console, you can schedule distribution using the **Scheduled tasks** window. The core server communicates the package's location (URL or UNC path) to the device, and the device then copies only the files or the portions of the files it needs from the delivery server.

For example, if you're reinstalling a software program because some of its files were corrupted or missing, the system copies only the damaged or missing files, not the entire program. This technology also works well over WAN links. You can store the package on multiple servers, and then schedule devices to use the server appropriate to their needs (that is, location proximity, bandwidth availability, and so on).

Software distribution will also resume interrupted package downloads. For example, if a mobile device was in the process of downloading a large package and that device disconnects from the network, once the device reconnects the download resumes right where it left off.

In Management Suite, software distribution consists of these main steps:

1. **Create or obtain a software package.** The software package can be one or more MSI files, an executable, a batch file, a Macintosh package, a Linux RPM package, or a package created with Management Suite's package builder. Put the package on your delivery server.
2. **Create a distribution package (Tools | Distribution | Distribution Packages).** The distribution package contains the files and settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, command-line parameters, additional files needed to install the package, and so on. These settings are stored in the database and create a distribution package. Once you create a distribution package, the information is stored in the database and can easily be used in multiple tasks.
3. **Create a delivery method (Tools | Distribution | Delivery Methods).** The delivery method defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Options include Targeted Multicast and push and/or policy distributions. Don't create a delivery method every time you want to distribute a package. Delivery methods allow you to define best practices for deploying software. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.
4. **Schedule the distribution job in the Scheduled tasks window (Tools | Distribution | Scheduled Tasks).** Here you specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.
5. When the scheduled time occurs, the scheduler service will start the scheduled task handler which deploys the package using the options selected in the delivery method. These may include:
 - If a delivery method that uses multicast is selected, multicast is used.
 - If a push delivery method is selected, the service contacts the software distribution agent on each device and informs it that the package is ready for installation.
 - If a policy base delivery method is selected, the package becomes available for download.
6. The software distribution agent obtains the package from its local cache, a peer on the network, or the delivery server and processes it on the device by installing or removing the packaged files.
7. After the package is processed, the software distribution agent sends the result to the core server, where it's recorded in the core database.

Separating distribution tasks into two parts, distribution packages and delivery methods, simplifies the distribution process. Now you can create delivery method templates that are independent of a particular package. For example, you could create a default Targeted Multicast delivery method template, and whenever you have a package you want to multicast, you can deliver the package using that template without having to reconfigure the distribution package or the delivery method.

If you have different people in your organization that create packages and distribute packages, these changes help simplify job roles and task divisions. Package creators can now work independently from package deliverers.

Understanding package types

Software distribution supports these package types:

SWD package

These are packages built with the Management Suite Package Builder (installed separately). For more information see "Building Packages."

MSI

These are packages in the Windows Installer format. You must use a third-party tool to create MSI packages. These packages consist of a primary .MSI file and can include supporting files and transforms. Transforms customize how MSI packages are installed. If your MSI package consists of multiple files, make sure you add all of them in the **Distribution package** dialog.

Executable

In order for an executable package to be used by software distribution, it must meet the following criteria:

- The executable must not exit before the installation is complete.
- The executable must return zero (0) for a successful installation.

As long as the executable meets these two criteria, any executable can be used for installing the package. You can include additional files for executable packages.

Batch file

Batch file packages are based on a Windows batch file. You can include additional files for these distribution packages. The successful completion status of the batch file package is based on the value of the errorlevel system environment variable when the batch file has finished running.

Macintosh

Any Macintosh file can be downloaded, though Management Suite won't download directories. Install packages (.PKG) can contain directories. They must be compressed. If the file downloaded has an extension of .SIT, .ZIP, .TAR, .GZ, .SEA, or .HGX, Management Suite will decompress the file before returning. (Users should make sure that Stuffit Expander* has its "check for new versions" option disabled; otherwise a dialog may interrupt script execution.)

Linux RPM

These are packages in Linux RPM format. These packages must be stored on a Web share for Linux RPM distribution to work.

Understanding the available delivery methods

Software distribution provides these delivery methods:

- **Push:** The packages may be multicast out to the managed devices. The core server then initiates package installation at the managed devices.
- **Policy:** The core server makes the packages available for download. When a managed device checks for available policies, the package will be returned. Depending on the policy type, devices may install the package automatically or make the package available to users for them to install when they want.

- **Policy-supported push:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it.
- **Multicast (cache only):** Multicasts the package to the target devices, no other action is taken on the managed device. The result is the package is cached locally on managed devices. Use this option to multicast the package to a few devices on each multicast domain. You can then create a task that uses the **Peer download (only install from cache or peer)** option. This allows you to regulate network bandwidth used for the distribution so it doesn't span multicast domains.

Software distribution core server components

The following components of software distribution run or reside on the core server:

- **LANDesk scheduled task handler:** This program (ScheduledTaskHandler.exe), launched by the scheduler service, starts a distribution job.
- **LANDesk scheduler service:** The console stores information about scheduled jobs in the database. The scheduler service (SCHEDSVC.EXE) monitors the information in the database to determine when tasks should be run.
- **Distribution package:** When you select a software distribution package in the **Distribution package** window, it stores this definition in the database. This definition is used by Management Suite when creating the commands that will be sent to the devices to install the packages.
- **Software distribution packages:** A package can be one or more MSI files, an executable, a batch file, a Macintosh package, a Linux package, or a package created with Management Suite's package builder. In most cases, the software package needs to contain everything necessary to install the application you're distributing.

For users of Management Suite versions prior to 8.5

Management Suite 8.5 reorganizes the way software distribution works in the Management Suite console. Software distribution is now divided into two parts:

- **Distribution packages:** Use this window to create distribution package. Once you've created a package or have an existing package you want to distribute, this window lets you configure the package for Management Suite.
- **Delivery methods:** Use this window to define how packages you've configured in the **Distribution packages** window will be delivered. For example, you can choose a Targeted Multicast distribution or a pull distribution.

If you've used versions of Management Suite prior to version 8.5, you'll also notice that application policy management is no longer on the **Tools** menu. Policy management is now part of the **Distribution packages** and **Delivery methods** dialogs. Legacy APM packages are upgraded to distribution packages, delivery methods, and scheduled tasks. Scripts remain unaltered.

Setting up the delivery server

The delivery server is the server that stores the software distribution packages. It can be either a Web server or a Windows NT/2000/2003 server. We recommend that for best results, the packages be URL-based. In general, properly configuring a URL is less work than configuring a UNC path.

Delivery server	Requirements
Web server	Microsoft Internet Information Server 5.0 or higher running on Windows NT or Windows 2000/2003, or any HTTP 1.1 compliant Web server with byte range support.
Network server	Windows NT 4.0 or Windows 2000/2003

To configure a Web server for software distribution

These steps explain how to create a virtual directory on a Web server and enable it for browsing. In general, virtual directories need to allow reading and directory browsing, and anonymous access to the virtual directory must be enabled. Execute must not be set or the share won't work correctly. You also may want to disable write permissions so devices can't change the directory's contents.

1. Create a directory on the Web server where you want to store your software distribution packages. The usual location for such a directory on an IIS Web server is a subdirectory in the c:\inetpub\wwwroot directory.
2. Copy the packages to this directory.
3. From the Control Panel, double-click **Administrative Tools** and then **Internet Services Manager**.
4. In the right panel, double-click the icon with the device's name and then click **Default Web Site**.
5. In an empty area in the right panel, right-click and select **New**, then click **Virtual Directory**.
6. From the wizard, click **Next** and then enter an alias for your directory. Click **Next**.
7. Either enter the path or browse to a path and click **Next**.
8. In the Access Permissions dialog, enable **Run script** and **Browse**. This enables you to browse packages when creating a distribution package. Click **Next** and **Finish**.
9. To enable **Port 80** on the Web server, in the left panel, right-click **Default Web Site**.
10. Click **Properties**. In the **Web Site Identification** dialog, the TCP Port box should display 80. If it doesn't, click **Advanced** to add the port.
11. Ensure that the Web site is available by opening a browser and entering the URL for your Web server and virtual directory. For example, if the name of your Web server is Test and the name of the virtual directory is Packages, enter the following URL:

```
http://Test/Packages
```

A list of the packages you have copied to this directory should appear.

The size and number of packages you put in this directory is limited only by available disk space. Subdirectories can be created to logically group packages. Each subdirectory that's created must have the access permissions set, as described in the To configure a Web server for software distribution task.

Once you copy the packages to a package share on a Web server, they're staged and ready to be copied to the target devices. When scheduled, the URL or UNC path of the package is passed to SDCLIENT.EXE (the device agent) as a command-line parameter. SDCLIENT.EXE manages the file transfer, starts the installation, and reports the status. Although the HTTP protocol is used for the file transfer, the status report is returned through the standard LANDesk agent.

The Web server communicates with the device to ensure that the package copies correctly. If the package transmission is interrupted during the download, the Web server can use the HTTP protocol to restart the download at the point where it stopped. The Web server doesn't check, however, to ensure that the package was installed correctly. That traffic is TCP-based, and it returns the status to the core server using the standard LANDesk agent.

To configure a network server for software distribution

Devices that don't have a browser must receive distribution packages from a UNC path on a Windows NT/2000/2003 network server. This can be the same folder as the one you set up on your Web server. For UNC path-based distributions to work correctly, you must enable a null-session share folder on your network server. Use the SYSSHRS.EXE utility to create a null-session share folder.

1. To set up a shared folder on your network server, right-click the folder you want to share and then click **Sharing**.
2. Click **Share this folder** and click **Permissions**.
3. Add the **Everyone** and the **Guest** groups, but grant them only read permissions. In a domain environment, also add the **Domain Computers** group and grant only read permissions. Apply the changes.
4. From your network server, click **Start | Run** and browse to the LDMAIN\Utilities folder on your core server.
5. Run the **SYSSHRS.EXE** utility. Although this utility states that it's for Windows NT devices, it also works on Windows 2000/2003 devices.
6. Check the shared folder you set up and click **Apply** and then **Close**.
7. Copy the software distribution packages to this folder on the network server.

The size and number of packages you store on the network server is limited only by the available disk space.

For more information about the SYSSHRS.EXE utility, download the SHARES.EXE package from <http://www.landesk.com/support/downloads/Resource.aspx?pvid=12&rtid=10> and extract the documentation.

Configuring IIS 6 Web servers for software distribution

Windows 2003 uses IIS 6 as its Web server. When hosting packages on an IIS 6 Web server, there is some additional configuration you need to do:

- Configure the virtual directory that hosts your packages.
- Register a MIME type with IIS.

IIS 6 handles virtual directories differently than IIS 5 (IIS 5 was the Windows 2000 Web server). On an IIS 6 server, if you select a directory and from its shortcut menu make it a Web share, the directory registers itself in IIS 6 as a Web application rather than a virtual directory. The problem is that as a Web application, when trying to select an executable file, the Web server attempts to run the file as a Web application rather than download the file to the user.

The resolution is to go into IIS, change the shared directory from a Web application to a virtual directory, and turn off execute permissions.

When hosting files on an IIS 6 server, files without a registered MIME file type will result in an HTTP error 404, File Not Found. This will result in the multicast and/or installation of the file failing unless you register MIME file types.

To register MIME file types

1. Launch Internet Information Services (IIS) Manager.
2. Expand the local computer in the tree.
3. Click **Web Sites | Default Web Site**.
4. From the package Web share's shortcut menu, click **Properties**.
5. Click the **HTTP Headers** tab.
6. Click **MIME Types**.
7. Click **New**.
8. In the **Extension** box, enter an asterisk (*).
9. In the **MIME Type** box, enter any name.
10. Click **OK** twice and apply the changes.

Distributing a package

A distribution package consists of the package file you want to distribute, any additional files needed by the package, and settings that describe the package components and behavior. You must create the package before you can create the distribution package definition for it.

These instructions explain how to create a software distribution package. For the package to execute correctly, the software distribution package must exist on either a network or Web server and the devices must have the software distribution agent installed.

There are three main steps required to distribute a package to devices.

1. Create a distribution package for the package you want to distribute.
2. Create a delivery method.
3. Schedule the package and delivery method for distribution.

To create a distribution package

1. Create the package you want to distribute.
2. Click **Tools | Distribution | Distribution Packages**.
3. From the shortcut menu of the package type you want to create, click **New distribution package**.
4. In the **Distribution package** dialog, enter the package information and change the options you want. Note that you must enter the package name, description, and primary file. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the package type and owner you selected.

To create a delivery method

1. If you've already configured a delivery method that you want to use, or you are using one of the default delivery methods, skip to the next procedure, "To schedule a distribution task."
2. Click **Tools | Distribution | Delivery Methods**.
3. From the shortcut menu of the delivery method you want to use, click **New delivery method**.
4. In the **Delivery Method** dialog, enter the delivery information and change the options you want. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the delivery method and owner you selected.

To schedule a distribution task

1. Click **Tools | Distribution | Scheduled tasks**.
2. Click the **Create software distribution** task toolbar button.
3. On the **Distribution package** page, select the distribution package you created.
4. On the **Delivery Methods** page, select the delivery method you want to use.
5. Click **Save** to save your changes.
6. From the network view, drag targets onto the task in the **Scheduled tasks** window. Targets can include individual devices, computer groups, LDAP objects, LDAP queries, and inventory queries.
7. From the task's shortcut menu, click **Properties**.
8. The **Target devices** page shows the devices that will receive this task.
9. On the **Schedule task** page, enter the task name and the task schedule.

10. Return to the **Overview** page and confirm the task is configured how you want it to be.
11. Click **Save** when you're done.

View the task progress in the **Scheduled tasks** window.

Working with distribution owners and rights

In environments where there are many Management Suite users, it can get confusing knowing which distribution packages, delivery methods, and scheduled tasks each user is responsible for. To help with this problem, Management Suite makes the user that created the distribution package, delivery method, or scheduled task the default owner of that item. Only the owner and RBA Administrators/Software distribution configuration users can see these private items.

Private items appear under the **My delivery methods**, **My packages**, or **My tasks** trees. Administrative users can see items for all users under the **User distribution packages**, **User delivery methods**, and **User tasks** trees.

When users create a distribution item, the **Description** page has a **Package owner** option. Users can select **Public** if they want all console users to see that item. Administrators can select a specific user in addition to **Public**.

Once a user has created an item, they can change the owner by clicking **Properties** on the item's shortcut menu. Once a non-administrative user sets an item to public, they can't make the item private again. Only an administrator can do that.

These RBA rights affect distribution item visibility:

- **Administrator:** Create and view public and private distribution items. Can view private distribution items for all users.
- **Software distribution configuration:** Create and view public and private distribution items. Can only see their private distribution items.
- **Software distribution:** View and use existing public distribution items and items owned by themselves. Can't create new distribution items.

About file downloading

Software distribution has several methods for getting the file down to the device for installation. These include:

- Obtaining the file from the multicast cache
- Obtaining the file from a peer
- Downloading directly from the remote source

When a file needs to be downloaded, the device software distribution agent, SDClient, first checks the cache to determine if the file is located in the cache. The cache is defined as either C:\Program Files\LANDesk\LDClient\sdmcache or the path stored in the "Cache Directory" under the multicast registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM\Distribution\Multicast
```

The structure of files in the cache will be identical to the structure of the files on the Web or network server. This allows multiple packages to have files with the same name and not cause problems.

If the file isn't in the cache, SDClient will typically attempt to download the file from a peer in the network. You can configure the delivery method to require a peer download.

If the file can't be obtained from a peer, SDClient will download the files directly from the UNC or URL source. You can configure the delivery method so that if the file is to be obtained from the source, only one device in the multicast domain will download the file from the source location. Under most circumstances when downloading from a UNC share, this requires the UNC share to be a NULL session share. If the file to be downloaded is URL-based, SDClient will download the file from the Web site.

In either case, SDClient will put the file in the multicast cache. After it is put in the multicast cache, SDClient processes the downloaded file.

When a file is downloaded into the cache it will remain in the cache for several days, but is eventually deleted from the cache. The amount of time that the file will remain in the cache is controlled by the delivery method used when deploying the package.

Configuring a preferred package server

You can specify the default server that devices will check for software distribution packages. This can be important in low-speed WAN environments where you don't want devices downloading packages from off-site servers. To set the preferred package server, add a string value to the following registry key on managed devices, and set the value to the preferred package server name. You can specify multiple package servers by separating them with semicolons.

```
HKEY_LOCAL_MACHINE\Software\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\PreferredPackageServer
```

Here's a sample registry entry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution]
"PreferredPackageServer"="Server1;Server2;Server3"
```

Before a package file (either primary file or an additional files) is downloaded remotely, this registry key is checked, and if the file is present on a preferred server (the servers are checked in the order listed, and only the server portion of the UNC or URL path will be replaced), the agent will download it from there. If the file isn't on the preferred server, it will be downloaded from the location specified in the distribution package.

The core server also supports the same registry key/value. When you set a PreferredPackageServer on the core, it tells the core to generate the package hashes from a server specified in the key. Specifying a local server makes the process much quicker. If the package isn't available on one of the PreferredPackageServers, the core falls back to generating the package hash from the path specified in the distribution package.

Typically, you should configure this key/value on the core when you're distributing large packages from a package server that's separated from the core by a low-speed WAN link. You generally won't want the core server pulling a large package over the WAN link for hashing, so hashing files on a server that's local to the core will be much faster and use less low-speed bandwidth.

Updating package hashes

Because many package files are obtained from peers in the network, the files are verified prior to installation. The integrity of the files are verified by comparing the MD5 hash of the file to the MD5 hash generated at the core server.

When a distribution package is first scheduled, Management Suite downloads the files and calculates the hash values associated with the primary file and any additional files used by the distribution package. If the hash stored with the package doesn't match the hash value SDClient computed on the target device, the download isn't considered valid.

If you make any changes to the package outside of Management Suite, such as updating the package contents, you need to reset the hash, or any scheduled tasks using the updated package will fail.

To reset a package hash

1. Click **Tools | Distribution | Distribution packages**.
2. From the shortcut menu for the package whose hash you want to update, click **Reset file hashes**. This can take a few minutes on large packages.

Using Targeted Multicast with software distribution

LANDesk Targeted Multicast technology makes it possible to distribute large packages to many users across the network with a minimum of network traffic. Targeted Multicast features require no additional hardware or software infrastructure, and require no router configurations to allow multicast packets. You get the extraordinary benefits of multicast technology with none of its traditional headaches.

Targeted Multicast is designed to work with your existing software distribution packages. When you use Targeted Multicast, you can easily distribute software, even in WAN environments with multiple hops and low connection speeds (56k). Targeted Multicast uses HTTP for delivery from a Web site to a subnet representative. Management Suite's inventory scanner provides all the subnet information to the Targeted Multicast service.

Targeted Multicast provides unique benefits that standard methods of "multicast" don't provide. Inventory-based targeting of devices enables you to send a package to a selected group of computers that fit specific criteria via a multicast. Targeted Multicast is also simplified because there's no need to configure routers to handle deliveries.

When compared to conventional software distribution methods, Targeted Multicast significantly reduces the time and bandwidth needed to deliver software packages. Instead of sending a package across the wire for each device, only one transfer is made for each subnet. Bandwidth savings increase as the number of devices on each subnet increases.

You can activate Targeted Multicast from the delivery method properties by checking the **Use Multicast to deploy files** option on the **Multicast** page of the **Delivery methods** properties.

Multicast is available in policy supported push, push, and multicast (cache only) delivery methods. Underneath the **Multicast** page you will find several pages that allow the multicast to be configured.

When you start a distribution using Targeted Multicast, you'll see the **Multicast software distribution** window. This window contains detailed information about how the distribution is proceeding. For more information about what each field means, click the **Help** button on the **Multicast software distribution** window.

Both Windows and Macintosh OS 10.2 devices support Targeted Multicast. Additionally, you can multicast OS deployment images.

Using peer download

Peer download is a Targeted Multicast option that forces targeted devices to install a package from the devices' local cache or from a peer on the same subnet. This option conserves network bandwidth, but for the package installation to be successful, the package must be in the local cache or a peer's cache.

If you don't select the **Peer Download** option, the Targeted Multicast device agent will still attempt to conserve bandwidth by checking the following locations for package files in this order:

1. Local cache
2. Peer on the same subnet
3. Package server

Copying files to the local multicast cache folder

You have the option of copying one or more files to the local multicast cache folder using multicast. This option copies a file to the target devices' local cache. It doesn't install the file or do anything else with it. This option is useful for getting files to multicast domain representatives or a device in each multicast domain. You can do an initial deployment to domain representatives and then redo the deployment with the peer download option to ensure devices only download the package from a peer on their subnet.

Configuring Targeted Multicast

Before using Targeted Multicast, you need to make sure the Targeted Multicast components are in place on the subnet you're distributing to. Targeted Multicast requires Management Suite 8 agents and a multicast domain representative.

To manually specify which computers will be multicast domain representatives

1. In the network view, click **Configuration | Multicast Domain Representatives**.
2. Add domain representatives by dragging the computers you want to be representatives from the network view into this category.

Targeted Multicast will use the first computer that responds per subnet in the **Multicast domain representatives** group.

Only Windows computers can be multicast domain representatives. If you are using multicast to distribute packages to Macintosh computers, make sure there is at least one Windows computer in the multicast domain that can act as a domain representative for the Macintosh computers. If you only have a few Windows computers in a predominantly Macintosh environment, it's best to manually specify Windows domain representatives in the Multicast Domain Representatives group.

You can throttle multicasts by changing the **Minimum number of milliseconds between packet transmissions** option in the **Packet timing** page under the **Multicast** page on the **Policy-supported Push, Push, and Multicast** delivery method windows.

You can also customize Targeted Multicast options in the Configure Management Suite Services dialog. To configure the Targeted Multicast service, click **Configure | Services | Multicast** tab. Click **Help** on that tab for more information.

About byte-level checkpoint restart and dynamic bandwidth throttling

Management Suite 8 and later versions support distribution byte-level checkpoint restart and dynamic bandwidth throttling. Checkpoint restart works with distribution jobs that SWD first copies to the device cache folder (by default, C:\Program Files\LANDesk\LDClient\SDMCACHE). When a bandwidth controlling option is selected, the files get copied to the device cache first, and checkpoint restart allows interrupted distributions to resume at the point where they left off.

Dynamic bandwidth throttling specifies that the network traffic a device creates has priority over distribution traffic. This option also forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you select this option and leave the **Minimum available bandwidth** percentage at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. Increasing the minimum available bandwidth preserves approximately the amount of device bandwidth you specify for distribution if the distribution needs network bandwidth and there is contention for bandwidth on the device.

If you're reinstalling or repairing an SWD package or an MSI package, you may not want to use the dynamic bandwidth throttling option, because these package types normally only download the files they need. Using dynamic bandwidth throttling in this case would force a full download of the package when a repair might normally only require a small portion of the package.

Dynamic bandwidth throttling isn't available on Windows 95, Macintosh, or DOS devices. Windows 98 and Windows NT devices can use dynamic bandwidth throttling if they have Internet Explorer version 4 or later installed.

You can configure collective bandwidth throttling so that only one device from the multicast domain will download from the remote source. You can also configure the amount of bandwidth used when downloading from the source. This feature is available on all versions of Windows systems. Collective bandwidth throttling isn't available on Macintosh or DOS systems.

Distributing software to Linux devices

Once you've deployed the Linux agents, you can distribute software to your Linux devices. The initial Linux agent deployment uses an SSH connection. Once the agents are installed, the core server uses the standard LANDesk agent to communicate with the Linux server and transfer files. To distribute software to a Linux device, you must have Administrator rights.

You can only distribute RPMs to Linux devices. The Linux agents will automatically install the RPM you distribute. The RPM itself isn't stored on the server after installation. You can install and uninstall the RPM you specify using software distribution. You can only use push delivery methods with Linux software distribution. For Linux software distribution, the settings in the push delivery method are ignored, so it doesn't matter which push delivery method you select or what the settings in it are.

The distribution follows this process:

1. The core server connects to the Linux device through the Standard LANDesk agent
2. The device downloads the package
3. The device runs a shell script that uses RPM commands to install the RPM package
4. The device sends status back to the core server.

You can store Linux RPMs on HTTP shares. Linux software distribution doesn't support UNC file shares. For HTTP shares, make sure you've enabled directory browsing for that share. If you use an HTTP share on a Windows device other than the core, you need to configure IIS with the correct MIME type for RPM files. Otherwise, the default MIME type IIS uses will cause the RPM to fail to download the file.

To configure the RPM MIME type on Windows devices

1. From Windows **Control Panel**, open **Internet Services Manager**.
2. Navigate to the folder that hosts your distribution files. From that folder's shortcut menu, click **Properties**.
3. On the **HTTP Headers** tab, click the **File Types** button.
4. Click **New Type**.
5. For the **Associated Extension**, type **rpm**. Note that rpm is lowercase.
6. For the **Content type**, type **text/plain**.
7. Click **OK** to exit the dialogs.

Once you've hosted the files on your package share, create a new Linux distribution package, associate it with the delivery method you want, and schedule the delivery.

Troubleshooting distribution failures

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, let the software sit for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll outs occur should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

Scheduled task can't find package

If the scheduled task indicates that the package can't be located, make sure that the package can be viewed from the device.

If the package is URL-based, you can check to make sure it is accessible by using a Web browser. Remember, if your DNS is set up to resolve the package, you'll need to verify that the package has been distributed to all of the Web servers.

If the package can be viewed from the device but still does not download properly, the problem may be that the URL or UNC based package share doesn't allow anonymous access. Check the permissions on the UNC or URL share and make sure it allows anonymous access. For UNC locations, make sure it has properly been configured as a null session share.

Bandwidth detection doesn't work

One of the most common problems that can occur is having PDS set up for bandwidth detection. In device setup, one of the common base agent options is to choose between PDS and ICMP for device bandwidth detection. When a device is configured to use PDS for bandwidth detection, it will only detect between RAS and non-RAS connections. So, if you configure a distribution to only work with high speed connection and the package installs on a computer with a WAN connection, check and make sure it is configured to use ICMP and not PDS.

Using policy-based distributions

LANDesk Management Suite enables you to manage sets of applications on groups of devices using policy-based management feature.

Read this chapter to learn about:

- About policy-based management
- Configuring policies
- Applying scope to application policies
- What users see on their devices
- Using the local software distribution portal

About policy-based management

Policy-based management (known as application policy management in earlier Management Suite releases) helps you easily manage sets of applications on groups of devices. Like any other scheduled task, policies require:

- An SWD package, MSI, executable, batch file, or Macintosh package that you create.
- A delivery method that supports policies, either policy or policy-supported push.
- Policy targets for the distribution packages, such as the results of an LDAP or core database query.
- A scheduled time at which the policy should be made available.

Policy-based management periodically reruns queries you have configured as part of the policy, applying your policies to any new managed devices. For example, perhaps you have a Department container in your LDAP directory that contains user objects. Any user whose Department object is "Marketing" uses a standard set of applications. After you set up a policy for Marketing users, new users who are added to Marketing automatically get the correct set of applications installed onto their computer.

Use the LANDesk Management Suite console to configure application policies, which are stored in the core database.

Policy-based management can deploy these file types:

- SWD packages
- Microsoft Installer (MSI) packages
- Single-file standalone executables
- Bat files
- Macintosh packages

Here's the task flow for policy-based management:

1. Make sure the software distribution agents are on your devices.
2. If you don't have a package for the application you want a policy for, create one. For more information, see "Distributing software and files."
3. Use the distribution packages window create a package definition for the package.
4. Create or select an existing policy-based delivery method.
5. Create a software distribution task in the **Scheduled tasks** window and select the package and delivery method from above.
6. Select the targets for the policy, this can include any combination of individual devices, database queries, device groups, LDAP items, and LDAP queries.
7. Schedule the task to run. When run, the distribution package will be made available for pull.
8. The policy-based management service on the core server periodically updates the policy target list by reevaluating the LDAP/database query results. This helps ensure that the core database has a current set of targeted users/computers.
9. A user logs on to a device, connects to the network, or otherwise starts the policy-based management agent.
10. The core server's policy-based management service determines the applicable policies based on the device's device ID and the logged-in user or LDAP device location.
11. The policy-based management service sends the policy information back to the policy-based management agent.

12. Depending on how you've configured the device to handle policies, the user selects the policies to run or the policies run automatically. Only recommended or optional policies are available in the list on the device. When an unprocessed recommended policy is in the list, it's checked by default. Periodic policies appear in the list once their execution intervals have lapsed. Selected policies execute sequentially.
13. The policy-based management agent sends the policy results to the core server, which stores the results in the core database. Policy-based management status is reported to the core server using HTTP for enhanced reliability. This status is reported in the Scheduled tasks window.

Configuring policies

Policy-based management an SWD package, MSI, executable, batch file, or Macintosh package for any policy you create. You can either create the packages ahead of time or you can create the packages while creating the policy. We recommend that you create the packages ahead of time to test them and ensure that they work before using them in a policy.

Normal distributions and policies can use the same distribution package. The difference is in the deployment, not the package creation. There are two delivery methods that support policy based distribution:

- **Policy delivery methods:** The policy-only distribution model. Only devices meeting the policy criteria receive the package.
- **Policy-supported push delivery methods:** The combined push distribution and policy model. First, software distribution attempts to install the package on all devices in the target list. This way, you can do an initial deployment using Targeted Multicast. Second, any devices that didn't get the package or that later become part of the target list (in the case of a dynamic target list) receive the package when the policy-based management agent on the device requests it.

The main difference between standard delivery methods and the policy-based delivery method is the policy-based **Delivery methods** dialog has a **Job type and frequency** page.

The job type and frequency options affect how target devices act when they receive the policy:

- **Required:** The policy-based management agent automatically applies required policies without user intervention. You can configure required policies to run silently. Any UI that appears on the device while a required task is installing should be non-blocking; in other words, the application being installed shouldn't require user input.
- **Recommended:** Users have the choice of when to install recommended policies. Recommended policies are selected by default on the device UI.
- **Optional:** Users have the choice of when to install optional policies. Optional policies aren't selected by default on the device UI.

You can also configure how frequently a policy can run:

- **Run once:** Once a policy successfully runs on a device, the device won't run that policy again.
- **Periodic:** When a recommended or optional policy is specified as being periodic, it will be removed from the UI when it's successfully processed and will be shown again in the UI after the specified interval has elapsed.
- **As desired:** Can be installed by users at any time.

To create a policy-based distribution

1. In the console, click **Tools | Distribution | Delivery methods**.
2. From the shortcut menu for either **Policy-based distribution** or **Policy-supported push distribution**, click **New delivery method**.
3. Configure the delivery method options you want. Click **Help** for more information on each page.
4. Set the **Job type and frequency** options you want.
5. Click **OK** when you're done.
6. Click **Tools | Distribution | Scheduled tasks**.
7. Click the **Create software distribution task** toolbar button.

8. Configure the task options you want and click **OK**.
9. With the policy-based distribution task selected, drag the policy targets to the right window pane.

Policy-based distributions take effect as soon as the policy task is started and there are targets resolved. Policy-supported push distributions take effect after the initial push-based distribution completes.

Adding static targets

Policy-based management can use static targets as policy targets. Static targets are a list of specific devices or users that doesn't change unless you manually change it. Add static targets by selecting individual devices from the network view as targets. Individual LDAP devices can't be added as static targets.

Adding dynamic targets

Policy-based management can use queries to determine policy targets. As of Management Suite 8, queries are stored only in the core database. For more information on queries, see "Using database queries."

Dynamic targets can include network view device groups, LDAP objects, LDAP queries, and inventory queries.

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct agent software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager and Scheduled Tasks Application Policy Manager.

Windows 95/98 and NT devices need to be configured to log in to the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require policy-based management application policy management. As of this printing, more information on installing Active Directory client support was available here:

<http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utls/dsclient.msp>

In order to target a device from LDAP, each Windows NT/2000/2003/XP device must have a computer account on the Active Directory domain controller. This means that the computer being used as the device must be logged in to the domain where the Active Directory exists. You can't simply map a network drive using the fully-qualified Windows NT domain name. The policy won't take effect this way.

To use Directory Manager to create a query

1. Click **Tools | Distribution | Directory Manager**.
2. Click the **Manage directory** toolbar button.
3. Enter the directory URL and authentication information and click **OK**.
4. Click the **New query** toolbar icon.
5. Create your query. For more information, see "Using LDAP queries."

Adding additional targets

When creating a policy-based task, it is often a good idea to initially deploy the policy to a small target set. This is done so that if problems are encountered when deploying the policy it will only impact a small set of users. Once the results of the deployment to the small set of users have been validated, add additional targets to the policy. When new targets are added to an active policy task, the policy immediately becomes available to the newly-targeted devices or LDAP items.

Applying scope to application policies

Multiple scopes can filter the policy-based management target details pane for a target lists. However, the final scope that a policy uses is always the scope of a task owner. If the policy task is listed in **Common tasks**, and another Management Suite user with a different scope looks at the target details pane for the task (let's call this second person a target list "editor"), the target details pane is filtered by the editor's scope. In this case, the editor may not see all the targets the policy will be applied to in the target details pane, because the editor's scope may not allow them to see all targets in the creator's scope.

What users see on their devices

Application policies are always processed using a pull model. Devices check with the core server for new policies that might apply to them. When this check occurs, a dialog appears at the device showing only unprocessed, recommended and optional policies, not required policies. When an unprocessed, recommended policy appears in the UI, it is checked by default to encourage the end user to process it.

Once a policy is processed, it may still show up in the UI if it's set up to run periodically. If this is the case, it will continue to be selected, even if it's a recommended policy. A policy may also continue to appear in the UI if it wasn't applied correctly.

Users can manually launch the policy-based agent by clicking **Start | Programs | LANDesk Management | Policy-based delivery**.

Using the local software distribution portal

The software distribution agent on managed devices also provides a software distribution portal. The portal checks the local software distribution cache for policies that apply to the local device/user. The portal then displays a Web page listing available policies. Users can select a policy from the list and click **Download selected** to install the packages associated with the policy.

To use the software distribution portal

1. On the managed device, click **Start | Programs | LANDesk Management | LANDesk software distribution portal**.
2. Click the policy you want to apply.
3. Click **Download selected**.

Building packages

This chapter explains how to use LANDesk Management Suite Package Builder to create software packages. You may also want to refer to "Appendix C: Additional Software distribution information."

Read this chapter to learn about:

- Setting up a package-building computer
- Package-building overview
- Running the Package Builder wizard
- Uninstalling software distribution packages

Setting up a package-building computer

The package-building computer should be a dedicated computer with a clean installation of its operating system. The clean installation is necessary because the package-building process captures all elements added or modified on the package-building computer.

Because you can distribute packages only to clients running the same operating system as the package-building computer, you should have a separate package-building computer, or a separate drive partition, for every operating system you distribute to. You can also use a single computer with multiple OS images as your package-building computer.

Any preinstalled software on the package-building computer reduces the Package Builder's ability to recognize changes. For this reason, your package-building computer must be as generic and clean as possible. This rule also applies to the CONFIG.SYS and AUTOEXEC.BAT files and other configuration files that the application installation process may modify.

To install the package-building software

1. From your package-building computer, browse to **ENUSETUP.EXE** in the LDMAIN\install\Package_Builder folder of the core server.
2. Double-click **ENUSETUP.EXE**, then click **Next**.
3. Type in the location of the folder where you want to install the package-building software, then click **Finish**.

Setup puts three items on the package-building computer:

- **Package Builder wizard:** Used to automatically create software distribution packages. It takes a "before" snapshot of the computer's state, has you install the software, takes an "after" snapshot of the computer's state, and builds a package from the differences in the snapshots.
- **Enhanced Package Builder:** Used to manually create, modify, and edit software distribution packages.
- **Package Builder wizard help:** Online help that describes the Package Builder wizard.

Once the Package Builder software is installed on your computer, you can use this computer to create and edit software distribution packages. The Package Builder stores packages on the local hard disk by default. Once these packages are built, you must move them from the package-building computer to the package share on your delivery server.

Package-building overview

You can use the Package Builder wizard to automate the process of taking snapshots and compiling them into standalone packages. As shown below, the process includes four steps:

1. Taking a pre-installation snapshot
2. Installing the application or making a computer configuration change
3. Taking a post-installation snapshot
4. Restoring the package-building computer

1. Taking a pre-installation snapshot

To build a software package, use the Package Builder to scan the local hard drive. You can specify exactly which portions of the drive are scanned in the Scanning Options page. This scan checks the system registry and all the directories and files on the local computer. After you install new software on the system, the Package Builder uses this information to detect what changes were made to the computer; it then compiles these changes to create the software distribution package. This information is stored in the Temporary Work Directory. Specify this directory in the Options page of the Package Builder wizard.

Package Builder scans all local drives by default. If you don't plan to make any changes to a local drive during the installation, remove it from the scan to speed up the pre-scan process. For best results, allow the Package Builder to scan the drive partition where the operating system is stored, plus the drive where you intend to install the software or change the configuration.

If, at any time during the package-building process, the hard drive space on the package-building computer gets low, the Package Builder will stop, display a warning, allow you to provide more drive space, then continue the package-building process.

Even if you remove all the local drives from the scan list, the Package Builder still scans the system files and folders, as well as the computer's registry.

2. Installing the application or making a computer configuration change

Once the pre-installation snapshot is created, the Package Builder prompts you to install the application software to distribute as a package.

You can install multiple applications in a single package, but you should install only suite-type applications with this process. If you install multiple applications as one distribution package and later want to omit one, you must first remove the entire group and then install a new group of applications. If you want to install multiple packages to your managed clients, you should edit the software distribution script so that it installs several different packages during the distribution.

The Package Builder monitors the installation during this step, then waits until the installation is finished to continue with the wizard pages. You can then customize the finished program. For example, if the install program creates an uninstall icon that you prefer not to distribute to clients, you can delete the icon before the post-installation snapshot in step 3, omitting it from the package. You can also add new icons to specific program groups, which provides a single point of access for all your users.

You need to provide any setup information requested by the system, and answer all questions presented during the software setup. The Package Builder cannot perform these tasks for you, but it will save the information as part of the package.

If you want to change only some of the system settings on clients, or if you want to copy a collection of specific files, you can create a package without using the snapshot process.

When you're satisfied that the application software or the configuration changes are ready, return to the wizard and click Next to start the post-installation snapshot.

3. Taking a post-installation snapshot

In this step, the Package Builder takes a second snapshot of the package-building computer and compares it with the pre-installation snapshot. By analyzing the differences, the Package Builder can identify any changes that have occurred on the computer, and then build a package distribution configuration script. This file has a .CFG file extension, and is located in the c:\Program Files\Intel\Package Builder\Working folder on the package-building computer.

This .CFG script file describes the changes to the registry, the file system, the desktop, and other system resources. It does not create a removal control file however, so you must add an uninstall option manually, either when you edit the script or when you schedule it for distribution.

Once these changes are saved, the Package Builder wizard offers the option to compile the .CFG file into an executable file, or to open it in Package Builder to make additional changes. Click Edit to open the new .CFG file in Package Builder and make your modifications. When you're satisfied with the installation, click Build to create the package.

Once finished, a page appears showing that the package was created and stored in the default directory on the package-building computer.

4. Restoring the package-building computer

Once you finish the package-building session, you should restore the package-building computer to its pre-installation state. This process ensures that the computer is in a clean state for the next package build. ESWD doesn't include a process for restoring the computer to a clean state; therefore, you should use a computer-imaging program such as the LANDesk imaging tool that is part of OS Deployment, Symantec's Ghost*, and so on to restore the client's operating system.

If you use a utility like Ghost to restore the package-building computer, you will also delete the .CFG file that was used to create the package. If you want to keep these files available, either to use in future packages or to edit at a later time, you can store them on a network share drive. Just specify a network location in the Options page of the wizard to preserve these files.

By default, each new system scan is stored in a new working directory, but you can use the same folder again if you prefer to overwrite the old system scan. Some users keep software images of multiple operating systems on a single package-building computer. This solution provides optimum flexibility when creating software packages, without dedicating multiple computers specifically for software package building.

Running the Package Builder wizard

As described earlier, building a software distribution package is a two-phase process. The first phase creates an installation script (.CFG file) in the Package Builder working directory. This script contains all the client instructions for installing the software. The second phase builds the software distribution package. The package contains the instructions plus the files.

To run the Package Builder wizard

1. From your package-building computer, click **Start | Programs | LANdesk Management | Package Builder wizard**.
2. Click **Scan Options** to configure the scan process. On this page, you can select which directories the wizard monitors for changes and whether the wizard creates a backup to return the client to its present state after the package has been created. When you're finished modifying the form, click **OK**.

At least one logical or physical disk drive must be monitored

The Package Builder wizard needs to monitor at least one logical or physical disk drive to track system information changes. If you clear the default drive selection in the Scan Options page, and set it to monitor no drives, the wizard will exit.

3. Click **Build Options** to configure user-specific settings for Windows NT and Windows 2000/2003/XP systems. You can select to have these settings applied to the logged-in user (or the default user if no one is currently logged in) or to all users. These user-specific settings include Start Menu items, shortcuts, and registry settings for the HKEY_CURRENT_USER key. To return, click **OK**.
4. Click **Next**. The wizard will check out your system.
5. Select the method you want to use to install the application:
 - If the installation program is locally available (such as a SETUP.EXE program), click **Browse** to locate the installation program, select it, and then click **Monitor**.
 - If the installation program is on an autorun CD, click **Next** and insert the CD.
 - To make other types of changes for a software distribution package (such as copying files or creating desktop shortcuts), click **Next** and run the appropriate utility.
6. Follow the prompts to install the software.
7. When the installation is complete, enter a name for the package. We suggest you enter a name that includes both the software and the operating system; for example, WinZip_Win2K for a package that installs WinZip on a Windows 2000/2003 client.
8. Click **Compare**.
9. When the .CFG file has been created, click **OK** and then **Build**.

Note: The .CFG file can be customized and then built into a package. For more information, see "Scripting guide for .CFG files" in Appendix C.
10. When the build completes, the wizard will put the package in the Onefile folder of the Package Builder Working directory. The package will be an .EXE file with the name you selected. Click **Finish**. You can manually test this package by clicking the .EXE file.

The next task is to set up the delivery server and copy this package to it. For more information, see "Setting up the delivery server."

Uninstalling software distribution packages

ESWD has the following methods for uninstalling packages that have been created and distributed to your clients:

- Uninstall command in Package Builder
- Uninstall option in the console
- Uninstall package with Package Builder wizard

Uninstall command in Package Builder

You can enable the Package Builder Uninstall command on all packages distributed to clients. If you use this command, packages create their own uninstall executable in the application's default directory on the client when they're installed. You can then create a script to activate that uninstall file on the client and remove the package.

Advantages to this method include:

- The uninstall is triggered by the script, and the installed files are completely removed.
- All file counters are correctly decremented during the uninstall. This means that shared .DLLs that affect other programs on the client aren't removed.

Disadvantages to using this method include:

- The Uninstall command must be included when you create the initial package.
- Uninstall prompts the user to remove the application. If the user responds "No," the package isn't uninstalled. You can't hide this prompt from users.
- The uninstall file is on the client, so a user could uninstall the software package without your knowledge. The uninstall file shows up in Control Panel | Add/Remove Programs.
- You must know the correct path to access the file.

The following example illustrates the syntax for creating a script that triggers the uninstall file to uninstall WinZip on the client:

```
[MACHINES]
REMEXEC0="C:\Program Files\WinZip\Uninstall\INSTALL.EXE"
```

REMEXECO is the Remote Execute command.

"C:\Program Files\WinZip\Uninstall\INSTALL.EXE" is the complete path to the uninstall file. Quotes are required if there are spaces in the path names. The default name for this file is "Uninstall" + the name of the software distribution package.

Once you have created a script that targets an uninstall package, schedule it to be sent to your users, and the package will be uninstalled.

Uninstall option in the console

You can use the tools in the console to uninstall distributed packages. From the console, click **Tools | Manage Scripts**, and click the **New Distribution Script** button. Select the .EXE package that installed the software. In the Create Script window, click **Uninstall**. This sets a "remove all" flag in the package so that everything installed in the installation script is removed.

The advantages of this method include:

- The uninstall executable is not on the client.
- This executable can uninstall software distribution packages that were not built with the Uninstall command.

Uninstall package with Package Builder wizard

If the above methods do not produce the desired results, there is one other option. You can use the Package Builder wizard to create a package of the uninstall process on the package-building computer, then distribute it to your clients.

This is not a recommended procedure

If the application you're uninstalling uses shared .DLLs, this method could remove .DLLs that are required by other applications.

To create an uninstall package

1. Start the **Package Builder wizard** on your package-building computer. The application you want to remove from your clients should be already installed with the same defaults as your clients.
2. Click **Next** to start the pre-snapshot phase, then click **Next** again. *Don't click the Browse button.* If you click Browse, you will start the installation process for another application; this procedure is for uninstalling an application.
3. When the pre-snapshot is complete, press **Alt+Tab** to switch to another application. *Don't click the Browse button.*
4. Click **Start | Settings | Control Panel** to display the Control Panel window.
5. Double-click the **Add/Remove Programs** icon to display the Properties dialog. In the **Install/Uninstall** tab, click the application you want to remove, and click **Add/Remove**.

If the application has its own uninstall program, you should run it now.

6. Once the application is uninstalled, press **Alt+Tab** to return to the Package Builder wizard.
7. Enter the **name** for this uninstall package, and click **Compare** to start the post-snapshot phase. Once this is complete, the Congratulations dialog appears. Click **OK** to close it.
8. When the Ready to Build dialog appears, click **Build**, then click **Finish** to complete the package-building process.

You can distribute this package to clients.

Using software license monitoring

Software license monitoring gives you the tools to implement complete, effective software asset management and license compliance policies.

IT administrators often find it challenging to track product licenses installed on numerous devices across a network. They run the risk not only of over-deploying product licenses, but also of purchasing too many licenses for products that turn out to be unnecessary. You can avoid these problems by using the **Compliance** tree to monitor and report on product licenses and usage across your organization. Compliance features include:

- **Passive, low-bandwidth monitoring:** The software monitoring agent passively monitors product usage on devices, using minimal network bandwidth. The agent continues to monitor usage for mobile devices that are disconnected from the network.
- **Reporting:** The power of compliance monitoring rests in its data-gathering capabilities. Use the data to track overall license compliance and to monitor product usage trends.
- **Product license downgrading:** For certain products, you can set up license downgrading so that newer versions of a product can loan a license to older versions, keeping your devices license compliant at all times.

Software license monitoring features include:

- Ability to scan for both known and unknown applications, and a disposition tool to define and track previously unknown applications.
- Application launch denial to keep unauthorized software from running even on devices disconnected from the network.
- Full integration with LANDesk asset management for current, complete information about installed applications.
- Extensive application usage and license compliance reporting.
- Extensive license monitoring and reporting features, including number of times each licensed application was launched, last date used, and total duration of application usage.
- Easy configuration of license parameters, including number purchased, license type, quantity and serial number.
- License purchase information, including price, date purchased, P.O. number, and reseller information.
- Installation tracking and reconciliation, including the license holder and physical location of the device the license is installed on, as well as additional notes.
- Aliasing to track software when vendor information or filenames change.

If you've used software license monitoring in Management Suite versions prior to 8.5, be aware of the following changes:

- Licenses are now tracked by group. For example, you can have the same product in different groups, and the licenses for that product will be tracked independently.
- In the **Compliance** tree, you can specify a scope for a product group. Products within that group will only count and report on licenses for devices that are within the specified scope.
- License management is done through the **Compliance** tree. The **All products** tree shows products you can manage and usage information for those products.

Read this chapter to learn about:

USER'S GUIDE

- Monitoring products for compliance
- How compliance monitoring works
- Configuring products to monitor
- Using scopes with products
- Denying product and file execution
- Creating product and vendor aliases
- Viewing license compliance and product usage/denial trends
- About LDAPPL3
- Exporting and importing software license monitoring data

Monitoring software license compliance

The **Software license monitoring** window is designed to let you monitor and manage the software that's installed on your devices. Navigate the window from the left pane, where you can see these categories in the **Software license monitoring** tree:

- **Compliance:** In this tree view, you can monitor usage and license compliance for products across your organization and view license compliance/usage for all devices. You can configure product licenses and define which devices are to be associated with product groups.
- **Denied products for all devices:** In this tree view, you can see all products you have denied access to. Managed devices won't be able to run these products.
- **All products:** In this tree view, you can see all predefined products and products you created. You can configure products by specifying which files they contain and setting up product license downgrading. Drag products from this view into the compliance view so you can configure them for monitoring.
- **Inventory:** In this tree view, you can edit the list of files the inventory scanner uses to identify your devices' software inventory. You can also specify those files that should be denied execution on your devices.
- **Aliases:** In this view, you can create product or vendor aliases. An alias ensures that you can correctly account for all installed executables from a specific vendor if the vendor name changes, or for a product if its vendor and name change. This feature is especially useful if you're monitoring products in the **Compliance** tree and need to maintain accurate information about your licenses.

You can also import and export data appearing in the **Software license monitoring** window for use on other Management Suite 8 core servers you may have on your network. This feature is useful if you need to ensure that software license monitoring information is synchronized on all of your version 8 core servers.

How compliance monitoring works

The software monitoring agent installs on your devices as part of the default device configuration setup. The agent records data about all installed applications on a device.

Use the **Software license monitoring** window to monitor installed applications. After you indicate the product files and licenses that you want to monitor, the following occurs:

- Management Suite detects devices that have the applications installed that you want to monitor and displays this list in the **Software license monitoring** window. The inventory scanner on managed devices updates usage information each time it runs.
- During the next scan, the scanner reads the usage data collected by the software monitoring agents and sends this data to the core server. Management Suite then updates the **Software license monitoring** window with information for the specific licenses and products you're monitoring.

About mobile devices

For mobile devices disconnected from the network, the software monitoring agent continues to record data and caches it. After the device reconnects to the network, the next scan detects and sends that data to the core server. The **Software license monitoring** window is then updated with the latest license compliance, usage, and denied application data for those mobile devices.

Configuring products to monitor

To begin monitoring products for license compliance and usage trends, you must complete four different procedures within the Software License Monitoring window:

1. Set up compliance groups
2. Associate files with products
3. Add product license information
4. Make the changes available to devices

Step 1: Setting up compliance groups

In the left pane under **Compliance**, set up a tree of product groups and individual products. You can group products any way you want, for example:

- By department
- By vendor/publisher, such as Adobe or Microsoft
- By specific categories, such as Unauthorized Files
- By product suite, such as Microsoft Office

Within these groups, add the products that you want to monitor for usage trends. For example, under an Adobe group, you might add products such as Photoshop* and Illustrator*.

The **Add products** tree view provides a list of preconfigured products you can use. When using a preconfigured product, you need to make sure the monitored files match the versions on your network.

To set up a compliance group

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. In the **Compliance** shortcut menu, click **New group**.
3. Enter the new product group name. If you're using scopes to define which devices are to be associated with the product group for the purpose of determining compliance, assign a scope to the group. For more information, see "Using scopes with products."
4. To add products under this group, right-click the group name and select one of the following:
 - **Add product:** To add an already defined product.
 - **New licensed product:** To add a new product, which will also appear in the **All products** tree view.
5. Enter the product name.

To edit compliance items

- To edit properties for a product: In the left pane, in the product name shortcut menu click **Properties**. Enter the product name, version, publisher name, if you want to deny its use to devices, and if you want to match all files (that is, require that all files associated with this product be installed on the device before a license is counted as used). Click **OK**.
- To delete or rename a product group or product: In the left pane, in the group or product name shortcut menu, click **Delete** or **Rename**.

Step 2: Associate files with products

By associating files with products, you define the files that must reside on a device in order for the product to be considered installed on that device and to be monitored.

By default, if any one file associated with a product is found on a device through the process of inventory scanning, then the product is considered to be installed on that device. If you want to require that all files associated with a product be found on a device in order for the product to be considered to be installed on that device, then use the **Match all** feature as described above in the "To edit compliance items" task.

You can select files to associate with products from categories under the **Inventory** tree. After you associate a file to a product, that file will also appear in the **Inventory | Views | In monitored product** category. When selecting files, you must pick versions that exactly match those found on your network. If the filename or size doesn't match, then the file won't be found and the product won't be monitored for compliance.

Software license monitoring puts files into these categories that you can select from:

- **Discovered but not in product:** Files that also appear in the discovered on computers list but aren't currently associated with a product. Use this list to view files that you may want to associate with a product for monitoring license compliance and usage trends.
- **Discovered on computers:** All files that have been discovered on your devices. You can sort the right-pane columns to get a clear understanding of each file's status, such as if it's associated with a monitored product, being scanned by the inventory scanner, etc. If discovered files have the status of **To be dispositioned**, this means they were discovered during a software scan but have not already been dispositioned to be scanned by the inventory scanner. A file must be dispositioned to be scanned by the inventory scanner before it is regularly scanned.
- **In monitored product:** Files that are associated with a product for monitoring license compliance and usage trends. You can't move these files from the **Inventory** tree; they're only shown for reference.

Alternatively, you can check the **All products** tree for preconfigured products. If a product there matches one you want to monitor, you can drag it to the **Compliance** tree and configure it there.

To associate files to a product

1. Browse to the desired product.
2. In the product's shortcut menu, click **Files**.
3. On the **Files** tab, click **Add**.
4. Use the **Find** box to enter a word, then use the **In column** drop-down menu to specify if the word is part of the file's vendor, product, or filename. You can also use the **File list** drop-down menu to specify the Inventory tree category you want to search.
5. Click the **Search** toolbar button.
6. Select the file or files from the returned list, then click **Add** to add it to the files list of this product.

If necessary, you can manually add files. For more information, see "Adding files to LDAPPL3."

After you have associated the files to the product, Management Suite detects the devices currently running the product (as indicated by the last software scan) and populates the **Software license monitoring** window with that information. After the next software scan, you can view the usage report to see devices that have run the product, or the denial report to see devices that have attempted to run the product.

To view a product usage report

- In the **Compliance** tree, from the product's shortcut menu, click **Usage report**.

To view a product denial report

- In the **Denied products for all devices** tree, from the product's shortcut menu, click **Denial report**.

You can also find out which products have the same version of a file associated with the by using the **Find in product** option.

To find which products have a file associated with them

1. Click **Inventory | Views | In monitored product**.
2. Find the file you want to search on, and from its shortcut menu click **Find in product**.
The cascading menu shows you which products have that same file and file version associated with them. Clicking a product takes you to that file in the product.

To find where files are installed on devices

1. Click **Inventory | Views | In monitored product**.
2. Find the file you want to search on, and from its shortcut menu click **Where installed**.

Step 3: Adding product license information

You need to add license information to a product for the product to be monitored for license compliance. If you only want to track product usage, you can skip this procedure.

After you set up license information for a product, if you ever see a red icon with an exclamation point appearing next to the product group, this means that one of the products in the group isn't license compliant. Expand the product group to find the non-compliant product, then view its associated information in the right pane.

To add product license information

1. Click **Compliance | product group | product**.
2. In the product's shortcut menu, click **Manage licenses**.
3. In the **Product licenses** dialog, use the tabs to enter the license, purchase, and tracking information that's relevant to your organization.
4. When finished, click **OK**.

Step 4: Making changes available to managed devices

You must use the **Make available to clients** button for any product changes to take effect on managed devices. Once you click this button, software license monitoring updates the product definition files. The next time devices do an inventory scan, the scanner gets the updated product definition files from the core server and applies any changes.

Tracking licenses using the Match all files option

You may encounter a situation where you need to track licenses for two or more products that contain an executable of the same name and size. In such a case, you also need to configure software license monitoring so it monitors a file unique to each product. By selecting **Match all files** and using both the executable and a unique file to identify license usage, you specify that all files associated with a product (as found in its **Files** list) need to be installed on a device before a product license is considered used. This ensures that the scanner can correctly track the products licenses.

The following two examples help explain when you would select **Match all files**:

- If you're tracking license usage for MSDE and SQL 2000, and they both use SQLSERVER.EXE of the same size, you should also track a .DLL or other application file that's unique to each product. Software license monitoring won't monitor these other files for compliance (only executables are monitored for compliance), but the unique file will help the scanner distinguish the MSDE license from the SQL 2000 license.

Note: If you add files whose extensions are different than .EXE to a product (in order to use the **Match all files** option), you must first edit the LDAPPL3.TEMPLATE file to include files having those extensions in a software scan. By default, LDAPPL3.TEMPLATE only specifies executables. For more information, see "Editing the LDAPPL3.TEMPLATE file "in Appendix A.

- If you're monitoring 10 licenses for Office XP Standard (that includes Word, Excel, Outlook, and PowerPoint), as well as 10 licenses for Office XP Pro (that includes the same applications, in addition to Access), you face the problem of wanting to monitor two distinct product licenses that contain executables of the same name and size. The scanner can't distinguish between license types by tracking individual files, nor by using just the **Match all files** option for both products.

In this case, you must go one step further by adding an Office XP Pro executable to the Files container of XP Standard (for example, Access), marking that executable as **Not in product**, and selecting **Match all files**. This ensures that the software monitoring agent won't record an Office XP Pro license as an XP Standard license, which would occur if only **Match all files** was turned on. Marking a file as **Not in product** tells the inventory scanner, which is responsible for recording license information for a device, that the file must not exist on the device for a license to be recorded for the product.

To mark an executable as not in product

1. Click **Compliance | product group | product**.
2. In the product's shortcut menu, click **Files**.
3. Select the file you want to search to exclude, and from its shortcut menu click **Not in product**.

Using scopes with products

The Management Suite administrator can create scopes to define sets of devices. A scope defines a set of devices from a database query, a directory location, or a device group. These scopes can be assigned to Management Suite users to limit the managed devices they can see while connected to a core server.

When connected to a core server, the Management Suite administrator can see every device managed by that core server. Management Suite users, on the other hand, are restricted and can only see the devices that reside within the scopes assigned to them. For more information, see "Using role-based administration."

With Management Suite 8.5 and later versions, you can now assign scopes to monitored products. In the Compliance tree, you can assign scopes to a product group. Products within that group will only count and report on licenses for devices that are within the specified scope.

For example, this allows you to group products by department and track licenses by department. If you didn't use scopes, and marketing had 50 licenses for WinZip and Engineering had 50 licenses for WinZip, you wouldn't be able to tell if engineering had exceeded their license and was borrowing from marketing.

With scopes, you can put the marketing and engineering devices in different scopes. You can then have marketing and engineering groups under the compliance tree, and include Winzip in both groups. Once you add the marketing and engineering scopes to their respective group, you'll be able to track the marketing and engineering licenses separately.

Before applying scopes to monitored products, you must create scopes in the **Users** window (**Tools | Administration | Users**).

To apply scope to a product

1. Put your products into groups that align with the scopes you want to apply.
2. From the shortcut menu for the group you want to apply a scope to, click **Scopes**.
3. Click **Add** and click the scope you want. Click **OK**.
4. In the **Scopes** tab, remove the **Default All Machines** scope. Deleting this allows the newly selected scope to be applied.
5. Click the **Refresh** toolbar button and verify the scope is working the way you want it to.

Downgrading product licenses

The **Software license monitoring** window lets you "downgrade" licenses for certain products: if you have two versions of the same product installed on your network, you can set up the newer version to loan licenses to the older version.

By exercising your downgrade rights, you can prevent the older version from exceeding its license count. For example, you could configure Office XP to provide licenses to Office 97 when Office 97 licenses are exceeded, ensuring that devices can still run Office 97 applications while staying within compliance.

This feature is useful only for products where the vendor permits license downgrading. Microsoft, for example, allows this for many of its products. To verify that license downgrading is permissible for a product, refer to your license agreements.

The following scenarios (in addition to the one mentioned above) describe when you can downgrade licenses:

- Product #1 loans licenses to products #2 and #3: For example, you could configure Office XP to loan licenses to Office 97 and Office 2000.
- Products #1 and #2 loan licenses to product #3: For example, you could configure Office 2000 and Office XP to loan licenses to Office 97.

To downgrade a product license

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.

2. Click **Compliance | product group | product**.
3. From the product's shortcut menu, click **Properties**.
4. On the **Downgrades** tab, click **Add**.
5. Select a product that you can give licenses to, then click **Add**.
6. To set up a second or third product to give licenses to, repeat step 3. The order in which the downgraded products appear in the list is important. Products ranked lower in the list will only get licenses if the products above them haven't used all of the available licenses. To move a product up or down in the list, select it and click **Move up** or **Move down**.

Only downgrade a product if your licensing for that product allows it.

You can monitor license downgrades in the product's **Manage licenses** dialog.

Denying product and file execution

You can prevent devices from executing products you specify. From a product's shortcut menu in the **All products** tree, you can click **Deny use of this product**. When devices try to run a denied product, they'll see a message box telling them their system administrator has prevented access to that program. You can restore normal access to a product by unchecking the **Deny use of this product** option in the **All products** tree. All denied products appear in the **Denied products for all devices** tree.

All files in the **Files** list of a denied product will be denied on devices. The **Match all files** product option state doesn't affect denied products.

You can also deny individual file execution. When denying individual file execution, note that the denial is based on filename only. Any filename matching a denied filename will be denied execution. To deny file execution, select the file you want to deny in the **Inventory | Files** tree and from its shortcut menu click **Deny use of this file**. This moves the file to the **Inventory | Files | To be denied** tree.

You must click the **Make available to clients** button for any product changes to take effect on managed devices.

Viewing license compliance and product usage/denial trends

One of the most powerful features of the **Software license monitoring** window is the ability to track overall license compliance and monitor product usage and denial trends. The following types of data appear in the right pane of the Compliance tree:

- **Overall license compliance:** Shows overall license compliance for all defined product groups
- **Product group license compliance:** Shows compliance at the product group level
- **Product usage report:** Shows usage information at the device level
- **Product denial report:** Shows denied executables at the device level

To view overall license compliance

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance**. In the right pane, overall compliance data for all defined groups will appear, such as:

- **Name:** Names of the defined product groups
- **Complies:** Shows if licenses are compliant for a product group
- **Out of compliance:** Number of out-of-compliance licenses for a product group
- **Licenses not deployed:** Number of licenses not being used for a product group
- **Licenses:** Total number of licenses available
- **Installations:** Number of installations detected
- **Loaned:** If license downgrading is active, how many licenses the product is loaning
- **Borrowed:** If license downgrading is active, how many licenses the product is borrowing

You can also click a product group to see compliance for a single group rather than all groups.

To view a product usage report

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance | product group**, and the product you want a report on. In the right pane, usage data for this product will appear, such as:

- **Device name:** Name of device
- **Last used:** Last time the .EXE was run on the device
- **Last user:** Username of last user to log in to the device
- **# Executions:** Number of times the .EXE has run on the device
- **Duration (minutes):** Number of minutes the .EXE has run on the device
- **Days since last used:** The last time the user started the product
- **Discovery date:** The date the product was first detected
- **Reset date:** When the usage history was reset last
- **Last reset date:** The last time the usage history was cleared from the core database and device registry. The date comes from the core server.

To view a product denial report

- In the **Denied products for all devices** tree, from the product's shortcut menu, click **Denial report**. In the right pane, denial data for this product will appear, such as:
 - **Device name:** Name of device
 - **Last user:** Username of last user to log in to the device
 - **# Denials:** Number of time the .EXE was denied.
 - **Last reset date:** The last time the usage history was cleared from the core database and device registry. The date comes from the core server.

You can sort these columns by clicking the column header. You can also double-click a device name to open a window showing the inventory on that device.

When you view product reports in the **Compliance** tree, the reports are filtered by the configured scopes. If you want to view a global report, view the report from the **All products** tree. From a product's shortcut menu in the **All products** tree, click **Usage** report.

Printing or exporting data in report format

You can print any of the Compliance tree data in report format or export it to a variety of file types, such as Crystal Reports*, Adobe Acrobat*, Microsoft Excel*, and so on.

To print or export data

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Compliance** and expand the tree to view the product data that you want to print or export. (This data will appear in the right pane.)
3. Click the **Print** toolbar button to open the data in report format.
4. To print the report, click the **Print** toolbar button.

Resetting usage and denial report data

You can clear the data for your monitored products' usage or denial reports. Clearing the data lets you reset the counter so you can begin tracking applications from a certain point on. The reset affects all devices, and it clears the device registries and the core database of all past usage and denial report data. For this reason, it's important to print or save any usage or denial reports you may want to keep before resetting. When you reset the usage and denial report data, you do so for all monitored products.

To reset usage and denial report data

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Right-click **Compliance** and select **Reset usage information**.
3. When prompted, click **Yes** to complete the reset.

On large databases, the reset can take a long time. If the reset times out, your DBA can reset the usage manually by entering the following SQL command:

```
UPDATE FileInfoInstance
SET SCM_TotalSessionTime = NULL,
SCM_SessionCount = NULL,
SCM_SessionsDenied = NULL,
SCM_LastUser = NULL,
SCM_LastSessionTime = NULL
```

Creating product and vendor aliases

Use the **Aliases** view to create product or vendor aliases. An alias ensures that you can correctly account for all installed products by:

- **Normalizing executable file data:** An alias lets you make consistent the information the core database needs to correctly identify an installed product. For example, the file information provided by a vendor isn't always consistent. Files scanned into the core database for various Microsoft products may show the vendor name as being Microsoft Corp, Microsoft (R), or just Microsoft. If you were to run a query on "Microsoft (R)" products, you would get only a partial list back of Microsoft products installed across your network. By creating a vendor alias of "Microsoft Corp" for all of your Microsoft products, you ensure that those products all have exactly the same vendor name.
- **Updating executable file data:** An alias lets you update file information if the product name or vendor changes after installation. For example, sometimes vendor or product names change because a company has been newly acquired or divested, or a company has renamed its product after several versions. If this occurs with your applications, use aliasing to associate new vendor or product names with the originals, ensuring that the core database can continue to identify your executables accurately. This feature is especially useful if you're monitoring products in the **Compliance** tree and need to maintain accurate information about your licenses.

About the Aliases view

The right pane of the **Aliases** view shows the original vendor and name for a product, as well as any new vendor and/or product names that you may have added. A software scan must occur before a new alias will appear in the **Software license monitoring** window or in Asset reports that include data about your device's software.

You can create two types of aliases in the **Alias properties** dialog:

- **Vendor:** An alias for all installed products of a certain vendor (enter the original vendor name and a new vendor name).
- **Product:** An alias for a specific product (enter original vendor and product names, as well as new ones). A product alias that includes a new vendor will always take precedence over an alias created for all products of a certain vendor.

Aliases you create will show up in the tree views for **Aliases**, **Compliance**, and **Inventory**, as well as in any asset reports that include device software data.

To create an alias

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. In the left pane's **Aliases** shortcut menu, click **Create alias**.
3. In the **Alias properties** dialog, enter the original vendor and original product name, as well as the new vendor and/or new product name for the application. Click **OK**.

To delete an alias

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. In the left pane, click **Aliases**.
3. In the right pane's **Aliases** shortcut menu, click **Delete**.

After you delete an alias, the core database reverts to using the original vendor and product name.

Editing software inventory

Use the **Software license monitoring** window's **Inventory** tree to configure the files you want scanned or ignored by the inventory scanner. The inventory scanner uses this configuration data to identify your devices' software inventory. The scanner recognizes software applications in three ways:

- Filename
- Filename and size
- Information included in an application's executable file

About the Inventory tree

The Inventory tree contains two panes that show the following details.

- **Left pane:** This pane shows a Files and Views tree.
 - **Files:** Displays the categories you can use to organize the files:
 - **To be scanned:** Files in your core server's LDAPPL3 that the scanner can identify on devices.
 - **To be dispositioned:** Files that have been discovered on devices but are unknown to the scanner. You must move these files into other categories before the scanner can identify them.
 - **To be excluded:** The scanner ignores all occurrences of a file that you move here. If you delete a file from **To be excluded**, it appears in the **To be dispositioned** category.
 - **To be denied:** Execution is denied for all occurrences of a file that you move here. End users who attempt to run a denied executable will see the program run for a few seconds before it closes down. If you delete a file from **To be denied**, it appears in the **To be dispositioned** category.
 - **Views:** Displays the following file lists in the right pane:
 - **Discovered but not in product:** Files that also appear in the **discovered on computers** list but aren't currently being monitored in the **Compliance** tree. Use this list to view files that you may want to begin monitoring for license compliance and usage trends.
 - **Discovered on computers:** All executables that have been discovered on your devices. You can sort the right-pane columns to get a clear understanding of each file's status, such as if it's in a monitored product, or if it's currently in one of the above file categories. If discovered files have the status of **To be dispositioned**, this means they were discovered during a software scan, but aren't in the **To be scanned** list. A file must be in the **To be scanned**, **To be excluded**, or **To be denied** list before it's regularly scanned, excluded, or denied on devices.
 - **In monitored product:** Files that are monitored for license compliance and usage trends in the **Compliance** tree. You can't move these files from the Inventory tree; they're only shown for reference.
- **Right pane:** This pane changes depending on the item you select in the left pane.

About LDAPPL3

LDAPPL3 is the new version of LDAPPL.INI that shipped with older versions of Management Suite. Unlike the past, you shouldn't edit this new file directly in a text editor, because the data is now stored in the core server's core database. The next time the server writes a new version of this file, changes made directly with an editor will be lost. All edits to software descriptions contained in LDAPPL3 must be made from the **Software license monitoring** window.

As shipped with Management Suite, LDAPPL3 contains descriptions of several thousand applications, providing a baseline of executables that your devices may have installed. Use this window to select the executables listed in LDAPPL3 that you want the scanner to identify, exclude, or deny on devices. If an executable isn't listed in LDAPPL3, you can add it. For more information, see "Adding files to LDAPPL3."

By default, LDAPPL3 contains descriptions of executables only. If you want the scanner to also identify other types of application files (.DLLs, .COMs, .SYSeS, and so on), you can manually add those files to any of the categories under the Inventory | Files tree *after* editing the LDAPPL3.TEMPLATE file to include all files of that type in a scan. For more information, see "Editing the LDAPPL3.TEMPLATE file" in Appendix A,

By default, the inventory scanner only scans for files listed in LDAPPL3. If you want to scan all files on devices, you can change the scanning mode to all files. Note that a mode=all scan mode can generate inventory scan files from devices that may be several megabytes in size. After the initial scan, the inventory scanner sends only delta scans, which will be much smaller. For more information on editing LDAPPL3, see "Editing the LDAPPL3.TEMPLATE file."

Distributing LDAPPL3 to devices

Beginning with Management Suite 8, The inventory scanner can use HTTP for LDAPPL3 file transfers. This allows the scanner to support Targeted Multicast features like polite bandwidth and peer download. Peer download allows devices needing LDAPPL3 updates will check with the core server for the latest version's date, then devices will broadcast to peers on their subnet to see if a peer has the update in its multicast cache. If a peer has the update, the file transfer happens on the local subnet without generating network traffic across routers or WAN links. For more information on Targeted Multicast and peer download, see "Using Targeted Multicasting with software distribution."

Editing LDAPPL3

By default, LDAPPL3 pre-populates the **Inventory | Files** categories of **To be scanned** and **To be excluded** when you set up Management Suite. From these categories, you can edit LDAPPL3 by using a file's shortcut menu to select a new category.

Once you edit the core's LDAPPL3, you need to make the most recent changes available to devices the next time they run an inventory scan. Do this by clicking the **Make available to clients** toolbar button. This action compresses the core's LDAPPL3 by 70 percent, which enables the scanner to update the devices' corresponding LDAPPL3 without using significant bandwidth. (The device's LDAPPL3 is installed as part of the default device configuration setup.) Both the device and core version of this file must be synchronized for the scanner to know which files to scan identify, exclude, or deny on devices.

If you don't want to wait for the next inventory scan to update your device LDAPPL3 files, you can make the edits available to devices in these ways:

- **By using your device logon scripts:** In the **Client setup** window, you can specify that your devices' local LDAPPL3 automatically receives updates from the core's .INI file each time a device boots.
- **By scheduling a job to push LDAPPL3 down to devices:** Use the **Scheduled tasks** window to schedule a time to push down the core's LDAPPL3 to each of your devices. By default, LDAPPL3 is located in the core's LDLogon shared folder.
- **By updating the LDAPPL3 automatically during inventory scans:** To automatically update the device's LDAPPL3 during an inventory scan, add a /i switch to the shortcut that launches the inventory scanner on devices.

To edit the core's LDAPPL3 file

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Inventory | Files**, then click **To be scanned** to view the list of files that the scanner currently detects on devices, or click **To be excluded** to view the list of files that the scanner currently ignores on devices. These are the two LDAPPL3 categories that are populated by default when you set up Management Suite.
3. In the right pane, scroll down to locate the files that you're interested in moving to another category. Or use the **Find** box to search for a file by entering a full or partial filename with the wildcard asterisk (*) and clicking the **Search** toolbar button. The correct file should appear in the list. You can edit LDAPPL3 by using a file's shortcut menu to select a new category.
4. Click the **Make available for clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the /i scanner command line parameter is used on devices.

Adding files to LDAPPL3

If you need to add new files to an LDAPPL3 category, you can do so by one of two methods.

To add individual files

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click **Inventory | Files**, then click the LDAPPL3 category the file should go into. See "About the Inventory tree" earlier in this chapter for descriptions of these categories.
3. Click the **New file** toolbar button.
4. In the **File properties** dialog, enter the filename and properties, or browse for the file. By selecting the file via browsing, the fields will automatically populate with the filename and size. When adding files to the excluded or denied lists, enter the file name. If you enter file size of 1, any file with that file name matches.
5. Click the **Make available for clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan.

If you want to add files other than executables with an .EXE extension, you must edit the LDAPPL3.TEMPLATE file and set the scanning mode to ALL. By running a Mode=ALL software scan, you can detect not only the device application files that are currently in LDAPPL3, but also all other executables that are unknown to LDAPPL3. The unknown files will populate the **To be dispositioned** category, where you can move them into other LDAPPL3 categories.

To run a Mode=ALL software scan, you must edit the LDAPPL3.TEMPLATE file located in the C:\Program Files\LANDesk\ManagementSuite\LDLogon folder of your core server. For more information, see "Editing the LDAPPL3.TEMPLATE file" in Appendix A.

Exporting and importing software license monitoring data

You can import and export data appearing in the **Software License Monitoring** window for use on other Management Suite 7 and 8 core servers you may have on your network. This feature is useful if you need to ensure that software license monitoring information is synchronized on all of your Management Suite 8 core servers.

You can *export* alias, product, and inventory data to an .XML file for importing into the core database on another core server.

You can *import* an .XML file from another console that you may have on your network. New data will be appended to the existing data. You can choose to overwrite or keep existing data in the core database.

To export LDAPPL3 data to an .XML file

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click the **Export** toolbar button.
3. Click **Only products and files** or **Everything**. Export products and files if you're sharing data with other core servers. Export everything if you're creating a software license monitoring data backup.
4. Enter or browse for the path and filename that you want to export to.
5. Click **OK**.

To import an .XML file containing LDAPPL3 data

1. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
2. Click the **Import** toolbar button and select an LDAPPL3 file or an .XML file that has the data you want to import into the core database on this core server.
3. Select whether you want to overwrite or keep existing data. Click **OK**.
4. Click the **Make available for clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the `/i` scanner command line parameter is used on devices.

Importing XML license data

You can import your organization's application license information into software license monitoring. The XML file must be in a specific format. Note that:

- All headings are required
- Product License Types must be spelled exactly including case and spacing
- All columns must have data
- The file must not be opened when importing
- You can create this file in a spreadsheet application and save it as an XML file

Here are the column headings:

- Product License Type
 - Competitive Upgrade
 - Freeware

- New Purchase
- OEM
- Product Upgrade
- Public Domain
- Shareware
- Unknown
- Quantity
- Serial Number
- Purchase Date
- Unit Price
- Order Number
- Reseller
- Owner
- Location
- Notes

Importing an old LDAPPL.INI into software license monitoring

The software description file in Management Suite 6.62 and older versions was named LDAPPL.INI. If you have a legacy LDAPPL.INI file containing software descriptions in the [Applications] and [Ignore] sections that you want to import into software license monitoring, you can, but the process is somewhat time consuming.

You must first edit the software descriptions in the [Applications] section that you want to import into the newer LDAPPL3. You can also import software descriptions from the [Ignore] section, which you don't have to edit before importing. Though the old LDAPPL.INI contained both software and hardware descriptions among other data, only the software descriptions from these two sections are imported into software license monitoring.

Importing customized hardware information

If you also have customized hardware information in the old LDAPPL.INI that you want to import (such as BIOS information), you must add that data to the LDAPPL3.TEMPLATE file directly. For more information, see "Editing the LDAPPL3.TEMPLATE file" in Appendix A.

There are two things you must edit in the old LDAPPL.INI to make the information compatible for importing into the newer LDAPPL3:

- In the [LANDesk Inventory] section—Update the Version and Revision lines
- In the [Applications] section—Use a comma to separate the vendor/product field for each application into two fields, one for vendor, one for product. For example:

In the old LDAPPL.INI, if a line reads:

```
<I>, EXCEL.EXE, 9165128, Microsoft Excel, 3.0a
```

You must change the line (by separating Microsoft (vendor) and Excel (product) with a comma) to read:

```
<I>, EXCEL.EXE, 9165128, Microsoft, Excel, 3.0a
```

IMPORTANT!

When importing software descriptions from an old LDAPPL.INI into the Software License Monitoring window, you must modify the data *exactly* as described. **Make sure you back up your database before starting the following procedure.** The better way to import software descriptions is to add the files individually to the categories under the Inventory | Files tree. For more information, see the procedure in the "Adding files to LDAPPL3" earlier in this chapter.

To import an old LDAPPL.INI into software license monitoring

Before starting this procedure, make a backup of your original LDAPPL.INI file.

1. Open your LDAPPL.INI in Notepad or another text editor.
2. In the [LANDesk Inventory] section of the file, search for the Version and Revision lines.
3. Change the **Version** line to read **3.0** and the **Revision** line to read **1.00**
4. In the [Applications] section of the file, edit the software descriptions that you want to import. Use the example shown above to ensure that you correctly edit the software description fields.
5. Delete all software descriptions from the [Applications] and [Ignore] sections that you don't want to import.
6. Save and exit out of the file.
7. In the console, click **Tools | Reporting/Monitoring | Software license monitoring**.
8. In the Software License Monitoring window, click the **Import** toolbar button.
9. In the **Files of type** box, click **LDAPPL3 Files**, then browse to the location of your saved .INI file.
10. Select the file, then click **Open** to import the edited software descriptions into the Software License Monitoring window. Verify that the software descriptions imported into these categories under the **Inventory | Files** tree:
 - From the [Applications] section to the **To be scanned** category
 - From the [Ignore] section to the **To be excluded** category
2. Click the **Make available to clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan.

Using unmanaged device discovery

Unmanaged device discovery (UDD) is new with Management Suite 8. UDD finds devices on your network that haven't submitted an inventory scan to the Management Suite core database. UDD has multiple ways of finding unmanaged devices.

- **Standard LANDesk agent:** Looks for the LANDesk CBA agent on computers. This option discovers computers that have Management Suite, LANDesk Client Manager, LANDesk System Manager, and so on.
- **Network scan:** Looks for computers by doing an ICMP ping sweep. This is the most thorough search, but also the slowest. You can limit the search to certain IP and subnet ranges. By default this option uses NetBIOS to try and gather information about the device. You also have an **IP FingerPrint** option, where UDD tries to discover the OS type through TCP packet responses. The **IP FingerPrint** option slows down the discovery somewhat.
- **NT domain:** Looks for devices in a domain you specify. Discovers members whether the computer is on or off.
- **LDAP:** Looks for devices in a directory you specify. Discovers members whether the computer is on or off.

UDD also supports these additional discovery methods. You must check either **Standard LANDesk agent** or **Network scan** before you can check one of these methods.

- **IPMI:** Looks for servers enabled with the Intelligent Platform Management Interface, which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.
- **Server chassis:** Looks for blade server chassis management modules (CMMs). The blades in the server chassis are detected as normal servers.
- **Intel* AMT:** Looks for Intel Active Management Technology-enabled devices. AMT devices appear in the **Intel AMT** folder.

To automate unmanaged device discovery, you can schedule discoveries to occur periodically. For example, you could divide your network into thirds and schedule a ping sweep for one third each night.

If you schedule a discovery, the core server does the discovering. Unscheduled discoveries happen from the console that starts it.

Unmanaged device discovery can't discover firewalled devices

Be aware that unmanaged device discovery usually can't discover devices that use a firewall, such as the Windows Firewall that is built into Windows XP. The firewall typically prevents the device from responding to the discovery methods that unmanaged device discovery uses.

Discovering unmanaged devices

It's easy to discover unmanaged devices.

To discover unmanaged devices

1. In the unmanaged device discovery window (**Tools | Configuration | Unmanaged device discovery**), click the **Scan network** button.
2. Select the discovery option you want.
3. Enter a starting and ending IP range for the scan. You must enter a range for **Standard LANDesk agent discovery** (CBA) or **Network discovery** to work. The range is optional for **NT domain** and **LDAP**.
4. Enter a **Subnet mask**.
5. Click the **Add** button to add the scan you just configured to the task list.
6. In the task list at the bottom of the dialog, select the scans you want to run and click the **Scan now** button to scan immediately, or the **Schedule task** button to run the scans later or on a recurring schedule. The **Scan now** and **Schedule task** buttons only run scans you've added to the task list and that are selected.
7. Watch the Scan Status dialog for scan status updates. When the scan finishes, click **Close** in the Scan Status and Scanner Configuration dialogs.
8. Click **Computers** in the UDD tree to view the scan results.

Configuring Windows NT domain discovery

UDD's Windows NT domain discovery option won't work unless you configure the scheduler service to log in to the domain with a domain administrator account.

To configure the Scheduler login account

1. Click **Configure | Services** and click the **Scheduler** tab.
2. Click **Change login**.
3. Enter a domain administrator username and password.
4. Click **OK**.
5. Restart the scheduler service so the change takes effect. On the **Scheduler** tab, click **Stop**, and once the service has stopped click **Start**.

What happens when UDD finds an unmanaged device

When UDD finds an unmanaged device for the first time, it tries to identify the device type so it can add the device to one of these four categories:

- **Chassis:** Contains blade server chassis management modules.
- **Computers:** Contains computers.
- **Infrastructure:** Contains routers and other network hardware.
- **Intel AMT:** Contains Intel Active Management Technology-enabled devices.
- **IPMI:** Contains servers that have the Intelligent Platform Management Interface.
- **Other:** Contains unidentified devices.
- **Printers:** Contains printers.

These four categories help keep the UDD list organized so you can more easily find the devices you're interested in. You can sort the device lists by any column heading when you click on a heading. UDD may not categorize devices correctly every time. You can easily drag misidentified devices to the correct group.

UDD tries to discover basic information about each device.

- **Device name:** The discovered device name, if available.
- **IP address:** The discovered IP Address. UDD always shows this.
- **Subnet mask:** The discovered subnet mask. UDD always shows this.
- **OS description:** The discovered OS description, if available.
- **MAC address:** The discovered MAC address, usually returned if the device has the standard LANDesk agent, NetBIOS, or if the device is on the same subnet as the core server or console that's doing the discovery.
- **Group:** The UDD group the device belongs to.
- **Standard LANDesk agent:** Shows whether the device has CBA on it. "Y" in the column means yes and "N" means no. You can deploy the Management Suite device directly to devices that have CBA loaded.
- **All users:** Users logged in at the device being scanned, if available.
- **Group/Domain:** The group/domain the device is a member of, if available.
- **First scanned:** The date UDD first scanned this device.
- **Last scanned:** The date UDD last scanned this device. This column helps you find unmanaged devices that may not be on the network any more or that were recently found.
- **Times scanned:** The number of times UDD scanned this device.
- **AMT:** Whether the device supports Intel Active Management Technology.

Depending on the device, UDD may not have information for all columns. When UDD finds a device for the first time, it looks in the core database to see if that device's IP address and name are already in the database. If there's a match, UDD ignores the device. If there isn't a match, UDD adds the device to the unmanaged device table. Devices in the unmanaged table don't use a Management Suite license. A device is considered managed once it sends an inventory scan to the core database. You can't drag devices from UDD into the main console network view. Once unmanaged devices submit an inventory scan, they'll be removed from UDD and added to the network view automatically.

If there's a discovered device that doesn't have all of its columns populated, you can select the device and click **Do IP Fingerprint**. UDD will send a series of packets to the device, and based on the response, try to identify more information about the device. Depending on the device and its OS type, IP fingerprint can find varying degrees of information.

You can create groups to further categorize unmanaged devices. If you move a device to another group, UDD will leave that device in that group if UDD detects the device again later. By keeping the main **Computers** group organized and by moving devices you know you won't be managing with Management Suite into subgroups or other categories, you can easily see new devices in the **Computers** group. If you delete a group that contains devices, UDD moves the devices to the **Other** group.

You can quickly find devices matching search criteria you specify by using the **Find** toolbar field. You can search for information in a particular column, or in all columns. Search results appear in the **Find results** category. For example, use Find to group unmanaged computers that have CBA by searching for "Y" in the Standard LANDesk agent field.

You can also create an AMS alert when UDD finds unmanaged devices. In AMS, the alert name to configure is **Unmanaged device found**.

Deploying to unmanaged devices

You can deploy Management Suite agents to unmanaged devices in one of these ways:

- Push-based deployments using scheduled tasks and a domain administrative account you've configured for the scheduler. Works for Windows NT/2000/2003/XP devices.
- Push-based deployments using the standard LANDesk agent. If the devices have the standard LANDesk agent, you can do a push-based deployment.
- Pull-based deployment using a login script.

For more information on deploying devices, see Phase 4 in the *Installation and Deployment Guide*.

When organizing devices for agent deployment, you may find it easier to sort the unmanaged device list by the standard LANDesk agent to group for standard LANDesk agent device deployments and to sort by domain for scheduled task deployments.

When deploying to Windows XP devices

Windows XP's default setting forces network logins that use a local account to log in using the guest account instead. If you aren't using a domain-level administrative account and are using a local account for the scheduler service, scheduled tasks will fail because the scheduler service won't be able to authenticate. For more information, see "Phase 4: Deploying the primary agents to devices" in the *Installation and Deployment Guide*.

To deploy agents to unmanaged devices

1. Click **Tools | Configuration | Agent configuration** and create a new configuration or use an existing one. From that configuration's shortcut menu, click **Schedule**.
2. Click **Tools | Configuration | Unmanaged device discovery**, and select the devices you want to deploy to. Drag the devices onto the **Scheduled tasks** window. If the **Scheduled tasks** window is a minimized tab, you can drag devices onto the **Scheduled tasks** tab, which opens the **Scheduled tasks** window.
3. If the devices don't have the standard LANDesk agent, click **Configure | Services**, and click the **Scheduler** tab. Make sure the scheduler account is one that will have administrative privileges on the devices you're deploying to.
4. Double-click the deployment script and set a start time. Click **OK** when you're done.
5. Watch the **Scheduled tasks** window for updates.

Restoring client records

Should you ever reset your core database and need to restore device data, you can use UDD to discover all devices on the network. You can then use the discovery results as the target for the "Restore client records" scheduled task.

If the devices have the standard LANDesk agent on them, this task has the devices send a full inventory scan to the core database that each device is locally configured for. The result of this task is those devices that have already been configured will be rescanned backed into the database and the devices will still be pointing to their correct managing core server. The task will fail on devices that haven't been managed by a core server.

To restore client records

1. Use UDD to discover unmanaged devices, as described earlier.
2. Click **Tools | Distribution | Scheduled tasks**.

3. In the **Scheduled tasks** window, click the **Schedule custom script** button.
4. Click **Restore client records**, and from its shortcut menu click **Schedule**.
5. From the UDD **Find results** tree, drag the computers you want restored onto the **Restore client records** task in the **Scheduled tasks** window.
6. From the **Restore client records** task's shortcut menu, click **Properties** and configure the task.
7. Watch the **Scheduled tasks** window for updates.

Using OS deployment

The LANDesk OS deployment and profile migration feature adds automated remote image deployment and device profile migration capabilities to your network. OS deployment and profile migration streamline new device provisioning and existing device migration, without requiring additional end user or IT interaction once the process starts.

You can schedule deployments and migrations to occur after hours, and by using the LANDesk Targeted Multicast technology to distribute images, you won't saturate network bandwidth by deploying the same image to multiple devices.

Note: For information on installing the OS deployment and profile migration component on your core server, and configuring your OS deployment and profile migration environment, refer to the *LANDesk Management Suite Installation and Deployment Guide*.

Read this chapter to learn about:

OS deployment

- OS deployment overview
- OS image guidelines
- Customizing images with Setup Manager and Sysprep
- Agent-based deployment
- Creating imaging scripts with the OS Deployment/Migration Tasks wizard
- Modifying scripts
- Multicasting OS images
- Viewing image status reports
- PXE-based deployment
- Using PXE representatives
- Booting devices with PXE
- Configuring the PXE boot prompt
- Using LANDesk managed boot
- Using the PXE boot menu
- Using the PXE holding queue

OS deployment overview

The OS deployment (OSD) feature provides two methods of deploying OS images to devices on your network:

- **Agent-based deployment:** Uses the device's existing Windows OS and installed LANDesk agents to deploy images. For more information, see Agent-based deployment later in this chapter.
- **PXE-based deployment:** Allows you to image devices with empty hard drives or unusable OSes. Lightweight PXE representatives eliminate the need for a dedicated PXE server on each subnet. For more information, see PXE-based deployment later in this chapter.

If you use Microsoft's Sysprep utility to create your images, OS deployment creates customized SYSPREP.INF files and injects them into each device's image on a per device basis, customizing Windows computer names, domain information, and so on from the core database.

OS deployment includes a built-in imaging tool you can use to create images. OS deployment also supports third-party imaging tools that you may already be using, such as Symantec Ghost* and PowerQuest DeployCenter*.

WARNING: OS deployment (imaging) should be used with caution. Operating system deployment includes wiping all existing data from a device's hard drive and installing a new operating system. There is a substantial risk of losing critical data if the OS deployment is not performed exactly as described in this document, or if poorly implemented images are used. Before performing any OS deployment, we recommend that you back up all data in such a manner that any lost data may be restored.

OS deployment steps

When planning and implementing an OS deployment operation, follow this sequence of steps:

1. (Optional) Run the Microsoft Setup Manager and Sysprep utilities on the device whose image you want to capture.
2. Create an image capture script with the OS Deployment/Migration Tasks wizard.
3. Schedule a task with the **Scheduled tasks** tool that runs the capture image script on the device whose image you want to capture. (Watch the Custom Job Status window updates for success or failure.)
4. Create an image deployment script with the OS Deployment/Migration Tasks wizard.
5. Schedule a task with the **Scheduled tasks** tool that runs the deploy image script on target devices where you want the image deployed.
6. Target devices running Windows OSes and LANDesk agents will begin the image deployment job when scheduled (agent-based deployment).
7. Target devices that are PXE-enabled will begin the image deployment job the next time they boot (PXE-based deployment).

Read the relevant sections below for detailed information about each of these steps.

OS image guidelines

You can create OS images with the LANDesk imaging tool or other imaging tools. When you run the OS Deployment/Migration Tasks wizard to create an imaging script, you are prompted to specify the image type and imaging tool. The wizard automatically generates command lines for the LANDesk imaging tool, Symantec Ghost 7.5, and PowerQuest DeployCenter 5.01.1.

Note: When you install the OS deployment and profile migration component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT.

If you have a different imaging tool, you can supply the command line for it at the end of the wizard. If you specify a custom command line, the wizard will put your custom line in the right location in the script so that you don't have to edit the script manually.

Image filenames

You should give your images unique filenames. Deploying different images with the same filename simultaneously on the same subnet can cause problems. Depending on how an imaging utility names image files, (multi-file Ghost images, for example), you may only have five unique characters in your filename once it is converted to a DOS 8.3 name format.

OS deployment creates image names using the first eight characters of the Windows computer name on which the image was created. If your image spans multiple image files, the imaging tool may only use the first five characters. When capturing images from multiple devices, you have two ways of ensuring that your images have unique names:

- Image one device at a time, renaming each image as it's created.
- Before running the job, ensure that the first eight characters (or five characters with multi-file images) of your image Windows computer names are unique.

Image file specifications and requirements

Regardless of the imaging tool you use, the compressed image size cannot exceed 2 GB because of DOS and disk imaging tool limitations.

OS deployment supports NTFS, FAT, and FAT32 file systems.

LANDesk agents and images

You should not include the LANDesk agents in your images. If you use a Sysprep image, OS deployment will install the LANDesk agents after the image is restored.

If your non-Sysprep images include LANDesk agents, you will need to delete the LDISCAN.CFG file from the root of the hard drive before imaging. You will also need to delete these keys:

- HKLM\Software\Intel\LANDesk\Common API\Unique ID
- HKLM\Software\LANDesk\Common API\Unique ID

If you leave these in the image, all devices using the image will have the same core database entry. Alternatively, if you have non-Sysprep images that already have LANDesk agents on them, you can enable the **Reject duplicate identities** option on the **Duplicate device ID** dialog (**Configure | Services | Inventory | Duplicate ID**).

Partitions and images

By default, when OS deployment restores an image on a target device, it deletes any preexisting partitions on that device.

The LANDesk imaging tool supports single-partition and multiple partition images (up to four partitions).

Non-Windows images

You can use OS deployment to deploy almost any image your imaging tool supports, not just Windows-based images. When deploying non-Windows or non-Sysprep images, make sure you do not select the **Image is Sysprepped** option on the **Configure imaging task** page of the OS Deployment/Migration Tasks wizard.

Customizing images with Setup Manager and Sysprep

You can use Microsoft's Setup Manager and Sysprep utilities when deploying Windows 2000 and Windows XP images. Sysprep customizes a Windows installation so that when the OS reboots, it looks for an answer file (SYSPREP.INF) and reconfigures itself for the new device. Setup Manager creates the SYSPREP.INF answer file that Sysprep uses.

Before creating OS deployment scripts, you should run Microsoft's Setup Manager (SETUPMGR.EXE) and create a SYSPREP.INF answer file for the images you're deploying. You can then use this file as the basis for any OS deployment scripts you create by selecting the **Use existing SYSPREP.INF file as a template** option on the **Specify Sysprep file information** page of the wizard. Any OS deployment script settings you make in the wizard override the equivalent options in the template SYSPREP.INF file.

Using Sysprep on your Windows 2000/XP images allows OS deployment to query the core database for each device you're deploying and to migrate certain user settings, such as:

- Windows computer name
- GUID (the unique identifier used to identify devices in the core database)

You can also set these options globally for images you deploy:

- Time zone
- Volume license key
- Registered name and organization
- Workgroup/Domain/LDAP Organizational Unit (OU)

OS deployment uses information from the core database and from the image deployment script to create a custom SYSPREP.INF for each device you're imaging. OS deployment then injects that SYSPREP.INF into each device's image.

Creating a Sysprep image

To create an image that uses Sysprep

1. On the device whose image you want to capture, make configuration or customization changes to prepare it for imaging.
2. At the root of the device's hard drive, make a c:\sysprep folder.
3. From a Windows 2000 or Windows XP installation CD, open \Support\Tools\DEPLOY.CAB and copy **SYSPREP.EXE** and **SETUPCL.EXE** to the sysprep folder you created.
4. Open a DOS command prompt and change to the sysprep folder. Run Sysprep. If you don't use the reboot option, you'll need to shut down the device from the Start menu once a message appears requesting that you shut down.
5. Boot to DOS and run your imaging tool manually.

For more information on Setup Manager and Sysprep

Refer to Microsoft's Web site for official documentation about the Setup Manager and Sysprep utilities. Sysprep has many powerful features you can use that are beyond the scope of this document.

Agent-based deployment

You can use the agent-based deployment method to deploy OS images to devices running Windows 98, Windows 2000, or Windows XP.

For information on the other method of image deployment, see PXE-based deployment later in this chapter.

Prerequisites

If you're not using PXE to deploy images, devices must meet the following criteria:

- Be in the core database if you have multiprocessor images.
- Have the standard LANDesk agent, Enhanced Software Distribution agent, and Inventory agent loaded. OS deployment uses the Enhanced Software Distribution agent to distribute images. If you'll be multicasting images, you also need to have the Targeted Multicasting agent loaded.

What happens during an agent-based deployment

1. The core server connects to the device and runs any preconfiguration commands you specified in the image deployment script.
2. OS deployment uses the Enhanced Software Distribution agent to distribute a virtual boot partition file to the device and modifies the boot sector to boot from this file, then reboots the device.
3. The device boots to DOS, detects and loads a network driver, then retrieves and installs the image file from the image server.

For non-Sysprep images, the device reboots after the imaging completes. OS deployment considers the job complete after this reboot.

For Sysprep images, agent-based deployment continues in this manner:

4. Before rebooting and loading the image, the DOS agent replaces SYSPREP.INF with a customized file for that device.
5. The imaged device boots and customizes itself based on what is in the SYSPREP.INF file.
6. Any post-image commands you specified in the image deployment script are run from the RunOnce registry key.
7. OS deployment runs WSCFG32.EXE using your default device agent configuration to reinstall the LANDesk agents.

Creating imaging scripts with the OS Deployment/Migration Tasks wizard

LANDesk OS deployment provides the OS Deployment/Migration Tasks wizard that lets you create both imaging (image capture and image deploy) scripts and profile migration scripts. All scripts are managed with the Manage Scripts tool (**Tools | Distribution | Manage scripts**).

For page-by-page descriptions of the wizard's interface, see Help for the OS Deployment/Migration Tasks wizard.

With the wizard you can create scripts that perform the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool, or a third-party tool such as Ghost, PowerQuest, or another tool of your choice.
- **Capture profile:** Creates a script that captures and stores a device's unique user settings, application and desktop settings, and files. You can also use this option to access the Collection Manager dialog to create a user-initiated profile migration package that can be run locally at individual devices.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Deploy image (with profile capture and restore):** Creates a script that performs a comprehensive deployment and migration job (capturing profile data, deploying an OS image, and then restoring the profile).
- **Restore profile:** Creates a script that restores previously captured profile data (user settings, application and desktop settings, and files) to target devices.
- **Generic DOS tasks:** Creates a script that runs DOS commands (including application launches) on devices.

Once you have created a script, you can schedule it to run on devices by using the **Scheduled tasks** tool.

Creating user-initiated profile migration packages

From the OS Deployment/Migration Tasks wizard, you can also access the Collection Manager dialog that lets you create a user-initiated profile migration package (a self-extracting executable file) that can be distributed and run on devices for user-initiated profile migration. For more information, see *Creating user-initiated profile migration packages*.

If you are deploying an image to PXE-enabled devices, you can add image deployment scripts to the PXE DOS boot menu. This menu is DOS-based and appears on the device during a PXE boot. For more information, see *Using the PXE DOS menu* later in this chapter.

To run the OS Deployment/Migration Tasks wizard

1. Click **Tools | Distribution | Manage scripts**.
2. In the Manage Scripts window, right-click **All OSD/Profile migration Scripts** and then click **New OSD/Profile migration script** in the shortcut menu to open the wizard. Or, in the Manage Scripts window, click the **New OSD/Profile migration script** toolbar button.
3. Select the type of script you want to create. For online help about options on any page of the wizard, click **Help**.
4. Advance through the wizard until you reach the last page. Click **Finish** to save the script and exit the wizard. Once complete, the script appears in the All OSD/Profile Migration Scripts group in the Manage Scripts window.

Administrators (users with the LANdesk Administrator right) can copy scripts to user subgroups in the Users Scripts group.

Additional notes on scripts

- Script names need to follow Windows file naming conventions. The wizard uses the script name you enter as the filename. If you use characters that aren't allowed in Windows filenames, you'll get an error about using invalid characters.
- All scripts are stored on the core server, in the \\<core>\LDMain\Scripts directory. If you have multiple consoles, the scripts will appear in the Manage Scripts window of each console.
- The wizard restores the settings on each page from the last script you created. If you change the script type from an imaging task to a profile migration task or a DOS task, the wizard clears the remembered settings.

About Generic DOS tasks scripts

- DOS scripts reboot the selected target devices and run the commands you've specified. These remote commands are sent one line at a time.
- DOS scripts run from the virtual boot partition and go through the same network detection process as normal OS distributions do.
- The "Abort this job if any command fails" option stops execution if one of the commands returns a non-zero DOS errorlevel code. You can view DOS task status in the Custom Job window or with a report.
- For more information about script commands, see Using Custom Scripts, a whitepaper located at <http://support.landesk.com>.

Modifying scripts

You can modify your scripts at any time, either by reopening the wizard and making changes, or by modifying the script directly in its .INI file and modifying any existing Sysprep settings in its associated .INF file.

Note: With DOS scripts, the only changes you should make are between the REMPINGx=DOS and REMEXECx=reboot.com lines. The other lines in the script manage the virtual boot partition files and boot process.

To modify a script via the wizard

1. Click **Tools | Distribution | Manage scripts**.
2. Right-click the script and click **Edit** in the shortcut menu (or double-click the script).
3. Advance through the wizard, making your changes.

To modify a script via an .INI file

1. Click **Tools | Distribution | Manage scripts**.
2. Right-click the script and click **Advanced edit**. The script's .INI file opens in Notepad. If this script has Sysprep settings associated with it, the SYSPREP.INF file also opens in Notepad.
3. Make your changes
4. Save the file(s).

Where .INI and .INF files are saved

.INI files are saved to the \\<core>\LDMain\Scripts directory. .INF files are saved to the \\<core>\LDMain\LANDesk\Files directory.

Multicasting OS images

This section discusses deploying images using the LANDesk Targeted Multicast technology. Multicasting is slower than a single distribution. Multicasting throttles bandwidth and stages the image on the target device's hard drive. However, multicasting to four or more devices will usually save enough bandwidth to make this worth it.

Targeted Multicasting supports only single-partition images, not multiple-partition images. Also, when using Targeted Multicasting with OS deployment, images can span up to 10 files.

When multicasting images, the image file is cached on the device before being restored. Your hard drive must have enough space for the image file and the restored files.

Before using multicasting with OS deployment, make sure the multicasting components are in place on the subnet to which you are distributing/deploying image files. Multicast OS deployments may fail if you don't specify domain representatives for each multicast domain in the console's **Multicast Domain Representatives** group. Multicasting requires LANDesk Management Suite 6.62 or higher agents on devices, and a LANDesk Management Suite 6.62 or higher multicast domain representative on the subnet.

If you try to multicast to a subnet that does not have a Multicast Domain Representative, the deployment will start but it will not be able to finish, and you will have to create an OSD boot floppy. For more information, see [Creating an OSD boot floppy](#). If your routers forward UDP-directed broadcasts, and there will be Windows devices that can act as multicast domain representatives on the subnet you're deploying the image to, you should be fine using Targeted Multicasting without designating multicast domain representatives. If your routers don't forward UDP-directed broadcasts, you must manually select your multicast domain representatives for each subnet, making sure the representatives you choose aren't among the devices you're deploying images to.

You can manually specify which devices will be multicast domain representatives by adding devices to the **Configuration | Multicast domain representatives** group in the console.

Make sure you don't image any multicast domain representatives in a subnet, because the imaging will fail and leave the devices in an unusable state.

You can throttle multicasts by changing the **Minimum number of milliseconds between packet transmissions** option in the **Configure advanced multicast options** page of the OS Deployment/Migration Tasks wizard.

WARNING: If your Multicasting environment isn't configured correctly and the Targeted Multicasting fails, all target devices may be unbootable unless you follow the directions above.

Setting the Maximum Packet Size for a Targeted Multicast with OSD

If multicast fails with distribution jobs, it may be because the maximum transmission unit (MTU) size on your network is fragmenting packets. Follow the steps below to adjust the MTU that multicast uses.

To set the Maximum Packet Size to 512 bytes for a Targeted Multicast script

1. Click **Tools | Distribution | Manage Scripts**.
2. From the script's shortcut menu, click **Edit**.

3. In the Multicast section of the script, add the following line at the end of the section.

```
MAX_PACKET_SIZE=512
```

This string will set the Maximum Packet Size for the Targeted Multicast to 512 bytes. Maximum Packet Size can be set to between 256 and 1464 bytes. A setting above this range, or no setting at all, will force the default setting of 1464. A setting below this range will default to 256 bytes.

4. Save and close the script.

WARNING: The MAX_PACKET_SIZE setting must be at least 28 bytes smaller than the Maximum Transmission Unit (MTU) for the network the package is being distributed on. This is determined by adding the size of the IP header (20 bytes) and the UDP header (8 bytes) that are sent with each packet of data. Setting the Maximum Packet Size higher than this limit will cause your distribution to fail.

Viewing image status reports

The device being imaged sends status updates to the core server. You can track status in the Custom Job window or with a report. As OS deployment sends imaging commands to devices, the commands appear in the Custom Job window. Devices being imaged send status updates for each script command that is sent. If image deployment fails for some reason, you can see the command that failed.

Common reasons why imaging fails include:

- Partition corruption
- Problems the imaging tool can't handle
- Network adapter auto-detection can't find a network adapter
- Undetectable network adapter you specified doesn't work. (If the network adapter driver you specify fails to load, that device will be stuck at the DOS prompt. You'll have to manually reboot it.)

OS deployment creates a status report for each job, showing if it failed or succeeded on targeted devices.

To view a status report

1. Click **Tools | Reports | All LDMS reports**.
2. Select the **OS deployment success rate** report.
3. From the list of log files, select the file for the job you're interested in viewing.
4. Click **Run**.

At the top of each report will be any jobs that failed on individual devices. Reports also show the details of each job, such as:

- **Machine Name:** For devices already scanned into the core database, this name will be the device name assigned to the device. For PXE-booted devices that haven't been inventory scanned, the machine name will be a MAC address. You can use a .CSV file to import MAC addresses into the core database. For more information, see Using CSVIMPORT.EXE to import inventory data.
- **Status:** Job status, either failed or OK.
- **Duration:** The amount of time each command took to complete.
- **Commands:** Each command that ran as part of the script. If a job failed, this column shows which command caused the failure.

PXE-based deployment

OS deployment supports PXE booting and image deployment. PXE-based deployment provides another method (in addition to agent-based deployment) of automated remote imaging of devices on your network. With PXE support, you can boot both new and existing PXE-enabled devices and either execute an OS deployment script at the device from a custom PXE DOS boot menu, or scan devices into your core database and then schedule an image deployment job with the **Scheduled tasks** tool.

PXE-based deployment is a quick and easy way to image devices in a variety of situations. For example:

- Initial provisioning of new devices
- Imaging devices in a test or training lab
- Re-imaging corrupted devices

LANDesk offers several options for using PXE to deploy OS images. For more information, see Understanding the PXE boot options later in this chapter.

PXE protocol basics

PXE (Preboot Execution Environment) is an industry-standard networking protocol that enables devices to be booted and imaged from the network, by downloading and installing an executable image file from an image server, before the device boots from the local hard drive. On a PXE-enabled device, the PXE protocol is loaded from either the network adapter's flash memory or ROM, or from the system BIOS.

PXE uses the following communication standards: DHCP (Dynamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol), and MTTFTP (Multicast Trivial File Transfer Protocol).

When a PXE-enabled device boots up, it sends out a DHCP discovery request. If a DHCP server implementing PXE is found, the server assigns an IP address to the device and sends information about available PXE boot servers. After completing the DHCP discovery process, the device contacts the PXE server and downloads an image file through TFTP. The imaging script is then executed, loading the OS image from the imaging server onto the device. The image file is referenced by an OS deployment script.

If you want to learn more about PXE and its underlying technologies and functionality, read the PXE Specification v2.1 located at <http://www.intel.com/labs/manage/wfm/wfmspecs.htm>.

Using PXE representatives

PXE support software is installed on your core server as part of the normal OSD installation. However, to enable PXE support, you must first deploy a PXE representative on each subnet of your network where you want PXE support available. PXE representatives provide scalability on your network by deploying OS images to devices in their respective subnets.

Devices on each subnet use normal PXE query and file transfer methods to communicate with their resident PXE representative, which communicates with the core server using Web services (HTTP).

Disable other PXE servers

If there is *any* other PXE server currently running on your network, you must first disable it in order to use LANDesk PXE support.

Deploying PXE representatives

You need to deploy one PXE representative on each subnet where you want to provide PXE boot support. You set up a PXE representative by running the PXE Representative Deployment script on the selected device. This predefined script is available in the Schedule Script dialog (**Tools | Distribution | Scheduled tasks** | click the **Schedule custom script** toolbar button).

You can have multiple PXE representatives on a subnet to help with load-balancing. When this is the case, the first PXE representative to respond to a device's request is the one that will be used to communicate with the core server.

Note: We recommend that you do *not* deploy a PXE representative on your core server.

There are no special hardware requirements for the device you select to be a PXE representative, but it must meet the following software requirements:

- **Operating system:** Windows NT 4, Windows 2000, or Windows XP.

For Windows NT and 2000, ensure that the Microsoft MSI service is running (XP includes MSI by default). If you have installed the latest service pack for either OS, MSI service should be running. Otherwise, you can deploy it to the target PXE representative from the console by following these steps: Click **Tools | Distribution | Scheduled tasks**, click the **Schedule script** toolbar button, select the **MSI service deployment** task, click **OK**, drag the target device(s) to the window, and click the **Set start time** button to schedule the MSI service deployment.

- **Installed LANDesk agents:** Enhanced Software Distribution agent and Inventory Scanner agent. For information about installing agents, see the *Installation and Deployment Guide*.

To deploy a PXE representative

1. In the console, click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar icon.
2. Select the **PXE Representative Deployment** script from the list, and from its shortcut menu, click **Schedule**.
3. In the console's network view, select the target device on which you want to install PXE services (in this case the core server).

4. Drag and drop the selected device to the **PXE Representative deployment** task in the **Scheduled tasks** window.
5. From the **PXE Representative deployment** tasks's shortcut menu, click **Properties** and finish configuring the task.

Updating PXE representatives

If you modify the PXE boot option settings (on the **Configure | Services | OS deployment** tab), you need to update all of your PXE representatives by re-running the PXE Representative Deployment script to propagate those changes to PXE representatives on each subnet. However, re-running the script is not necessary if you simply move PXE proxies from the Available proxies list to the Holding queue proxies list. For more information about the PXE holding queue, see Using the PXE holding queue later in this chapter.

To update or remove a PXE representative

1. Click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar icon.
2. To update a PXE proxy, select the **PXE Representative Deployment** script from the list, then click **OK**. Or, to remove a PXE proxy, select the **PXE Representative Removal** script, then click **OK**.
3. Drag and drop the target device(s) to the appropriate task in the **Scheduled tasks** window, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Booting devices with PXE

When a PXE-enabled device boots, the following occurs:

1. The PXE-enabled device sends out a query for PXE services running on a PXE representative on the network.
2. If a PXE representative exists on the subnet, it responds and tells the device to continue to boot using PXE.
3. A PXE boot session is initiated on the device and the PXE boot prompt displays. The default prompt message displays for four seconds and says "Press F8 to view menu." (You can modify these PXE boot prompt settings on the **Configure | Services | OS deployment** tab.)
4. If the **F8** key is pressed before the countdown expires, a preliminary PXE boot menu appears, allowing you to choose from the following boot options:
 - **Local boot:** The device boots to the local hard drive. If no OS is present, an error message appears.
 - **LANDesk managed boot:** The device is added to the console's network view (displays the device's MAC address), where you can schedule an OS deployment script to run on it.
 - **LANDesk boot menu:** The device displays the boot menu you created with the PXE Boot Menu tool, and you can select an OS deployment script to run on it. For more information, see Using the PXE Boot Menu later in this chapter.
5. If you don't press the **F8** key before the countdown expires, the device will use the default boot option. The default boot option is determined by the following conditions:
 - If the device detects a scheduled imaging job for itself in the core database (either a failed or pending job), the default boot option becomes **LANDesk managed boot**.
 - If the device does *not* detect an image job for itself, the default boot option becomes **Local boot**.
 - The **PXE DOS menu** will never become the default boot option.
6. The scheduled OS deployment script runs on the device.

Understanding the PXE boot options

This section provides information on configuring the PXE boot prompt, and how to use the following PXE boot options:

- LANDesk managed boot
- PXE Boot menu
- PXE holding queue

Configuring the PXE boot prompt

You can control how the PXE boot prompt behaves when devices attempt to PXE boot.

When a PXE-enabled device boots up, a DHCP request attempts to initiate a PXE session by looking for a server (or proxy) running PXE services software (PXE and MTFTP services). If the device discovers a PXE server, the PXE boot prompt displays on the device for a specified number of seconds. By pressing the F8 function key during this countdown, you access the PXE boot menu and can select an OS image to deploy on the device.

Note: If you have PXE representatives running on subnets of your network, and you want to implement PXE boot prompt changes to any of those proxies, you must run the PXE Representative Deployment script on the proxy.

To configure PXE boot prompt options

1. Click **Configure | Services**, then click the **OS deployment** tab.
2. Enter a value (in seconds) in the Timeout option. The default value is 4 seconds. The maximum number of seconds you can enter is 60 seconds.
3. Type a message in the Message text box. The default message is "Press F8 to view menu." The maximum number of characters you can type is 75 characters.
4. Click **Apply** to save your changes, or click **OK** to save your changes and close the dialog.

To implement PXE boot prompt changes to a PXE representative

1. Click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar button.
2. Select the **PXE representative deployment** script from the list, then click **OK**.
3. Drag and drop the PXE representative from the network view onto the task.
4. Select the **PXE representative deployment** script, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Using LANDesk managed boot

LANDesk managed boot is the default boot option when a PXE-enabled device boots and detects a failed image deployment script or failed DOS task script for it in the core database. You can also select this boot option manually at the device when the boot option menu appears.

Because it allows unattended deployment, LANDesk managed boot is useful for pre-targeting devices for imaging. For example, you could pre-target new devices for a particular OS image even before they arrive by importing a .CSV file containing device MAC addresses into the core database. For more information, see Using CSVIMPORT.EXE to import inventory data.

To pre-target devices with the LANDesk managed boot option

1. Before the PXE-enabled devices are connected to the network, add their identifications to the core database by importing a .CSV file.
2. Schedule an image deployment job for the devices.
3. The imaging job fails because the devices are not yet connected to the network.
4. Connect the devices to your network and boot them.
5. The devices detect a failed imaging job and default to the LANDesk managed boot option.
6. The previous failed image deployment job automatically launches and images the target devices.

Using the PXE boot menu

The PXE boot menu lets you interactively select an image deployment script for a device without having to schedule an image deployment job. This method might be useful when you have to re-image corrupted devices. Before using the PXE boot menu, you must first configure it by adding the OS deployment scripts you want to display in the menu.

You build the PXE boot menu system by creating directories and placing pre-configured OS deployment scripts in those directories. The script's description appears as a menu item in the PXE boot menu on the device.

To configure the PXE boot menu

1. Click **Tools | Distribution | PXE boot menu**.
2. To add a new directory or subdirectory to the menu system, click the **New** toolbar button (or right-click the parent directory and select **New**).

Note: Subdirectories can extend four levels from the top directory.

3. Type a name for the directory. For example, the directory name could describe the OS platform or version number of the images contained in that directory. You can also change the name of the directory at any time by clicking the **Rename** toolbar button (or right-clicking the directory and selecting **Rename**).
4. Click **Tools | Distribution | Manage scripts**, then drag and drop image deployment scripts to the appropriate directory in the PXE Boot Menu window.

Note: A maximum of 18 scripts can be placed in each directory.

5. To save the PXE boot menu, click the **Update** toolbar button. (Note that you must click the Update button here in the console if you want changes to appear in the PXE boot menu on PXE devices when they boot.)

To access the PXE boot menu from a device

1. Boot a PXE-enabled device.
2. When the PXE boot prompt displays, press the **F8** key before the countdown expires. Select **PXE DOS menu**. The menu system that you configured in the console's PXE Boot Menu window appears.

3. To open a directory and view its subdirectories and images, type the number of the directory and press **Enter**. Navigate the menu system and find the image you want deployed on the device. You can press **B** to go back one level, or press **X** to exit the menu system.

Note: If you exit the menu system without making a selection, the device will wait for a scheduled imaging job from the core server.

4. To select an OS image (referenced in an OS deployment script), type the number of the script and press **Enter**. The script runs and the image is loaded on the device.

Using the PXE holding queue

The PXE holding queue is another method for remotely deploying OS images to PXE-enabled devices. This method is especially useful in these situations:

- In a controlled lab environment where you frequently need all devices re-imaged with an identical image.
- For imaging "bare-metal" devices in a lab that can then be moved into their appropriate production environment.

By designating a subnet's PXE representative as a PXE holding queue, all the PXE-enabled devices on that subnet will be automatically added to the PXE holding queue in the console's network view when they PXE boot. You can also add a device to a PXE holding queue by scheduling the PXE - Add to Holding Queue script on the device, or by copying the device directly into the PXE holding queue group in the network view. Devices can then be scheduled for an image deployment job.

To configure a PXE holding queue

1. Set up PXE representatives on your network.
2. Click **Configure | Services**, then click the **OS deployment** tab.
3. Select and move PXE representatives from the Available proxies list to the Holding queue proxies list.

The Available proxies list shows all available PXE representatives on your network, identified by device name. This list is generated by running an inventory scan that detects PXE software (PXE and MTFTP protocols) running on the device. The inventory scan is run automatically whenever a PXE representative is initially set up.

4. Click **Reset**. The Reset button forces all PXE-enabled devices on the same subnet as the selected PXE representative to re-enter the PXE holding queue in the console's network view. These devices can then be scheduled for an imaging job.

Note: The Reset button is enabled when you select a PXE representative in the Holding queue proxies list.

5. Click **Apply**, then **OK** to save your changes and close the dialog.

The next time a device on that subnet boots, it will be added to the PXE holding queue object in the console's network view.

To deploy an image to a device in the PXE holding queue

1. Click **Tools | Distribution | Scheduled tasks**, then click the **Schedule custom script** toolbar button.
2. Select an OS deployment script from the list, then click **OK**.
3. In the console's network view, open the **PXE holding queue** object, then select the target devices you want to deploy the image to.
4. Drag and drop the selected devices to the **Scheduled tasks** window, and from the task's shortcut menu, click **Properties** and finish configuring the task.

Using profile migration

LANDesk's profile migration feature adds device profile migration capabilities to your network. OS deployment and profile migration streamline new device provisioning and existing device migration, without requiring additional end-user or IT interaction once the process starts.

You can schedule deployments and migrations to occur after hours, and by using the LANDesk Targeted Multicast technology to distribute images, you won't saturate network bandwidth by deploying the same image to multiple devices.

Note: For information on installing the OS deployment and profile migration component on your core server, and configuring your OS deployment and profile migration environment, refer to the *LANDesk Management Suite Installation and Deployment Guide*.

Read this chapter to learn about:

Profile migration

- Profile migration overview
- Profile content
- Creating collections
- Migrating user accounts
- Migrating application settings, templates and associated files
- Migrating Desktop (PC) settings
- Migrating files and folders
- Creating file rules
- Creating migration scripts with the OS Deployment/Migration Tasks wizard
- Creating user-initiated profile migration packages
- Running user-initiated profile migration packages

Profile migration overview

Profile migration complements OS deployment by offering a complete deployment and migration solution. With profile migration, you can preserve the customized desktop and application settings, and personal data files, for all of your users during an upgrade or migration project. Profile migration supports in-place migrations of individual devices as well as remote, large-scale migrations of multiple devices across your network.

Profile migration can best be understood as a two-part process:

1. *Capturing* a source device's unique profile, consisting of user accounts, desktop (PC) and application settings, and data files.
2. *Restoring* the profile to a target device.

For step-by-step descriptions of the profile capture and restore procedures, see [Creating migration scripts with the OS Deployment/Migration Tasks wizard](#).

For page-by-page descriptions of the wizard's interface, see [Help for the OS Deployment/Migration Tasks wizard](#).

Migration methods: scripted and user-initiated

Using profile migration, you can create separate capture and restore scripts with the OS Deployment/Migration Tasks wizard. The script can then be scheduled to run remotely on one or multiple target devices on your network.

Additionally, at the console, you can create self-extracting executable files (called user-initiated packages) that you, or the end user, can run directly from individual devices as a user-initiated profile migration. The user-initiated package launches a program called the LANDesk profile migration wizard. For more information, see [Creating user-initiated profile migration packages](#) later in this chapter.

The purpose of these two migration methods is the same; however, there are some differences in functionality. For example, the in-place user-initiated method lets you select which user accounts to migrate, while the scheduled script method does not. The information below refers specifically to the script method. The OS Deployment/ Migration Tasks wizard includes its own online help that describes the functionality of that utility. When running the wizard, click Help on any of the wizard's pages for more information.

Migration paths

Profile migration supports migrating across Windows operating system versions as follows:

- From Windows 95 and 98 SE ...to Windows 2000 SP3 or Windows XP
- From Windows NT 4 ...to Windows 2000 SP3 or Windows XP
- From Windows 2000 ...to Windows 2000 SP3 or Windows XP
- From Windows XP ...to Windows XP
- Windows Server 2003 is also supported (for both capture and restore)

Prerequisites

To do a profile migration, devices must meet the following prerequisites:

- Devices must be scanned in the core database.
- Devices must have the standard LANDesk agent (that includes the inventory scanner and local scheduler) and Software distribution agent installed. Profile migration uses the Software distribution agent to distribute files.

Profile content

Profile migration allows you to migrate the following content:

- User accounts
- Application settings, templates, and associated files
- Desktop (PC) settings
- Files and folders

User accounts are migrated by default. Settings and files are migrated according to a user-defined collection of rules (see Creating collections below for more information). You can create rules for applications, desktop settings, and files and folders.

Creating collections

Use the Collection of Rules dialog to create new collections and edit existing ones. A collection is a user-defined set of application, desktop, and file rules that determines the profile content to be migrated (captured or restored) by the migration script.

To create a collection

1. To access the Collection of Rules dialog, first click the **Collection manager** button on the Manage Scripts window's toolbar, then select **Collections** and click **New**. Or, through the OS Deployment/Migration Tasks wizard, by clicking the **Manage** button on the Select a collection for this profile page of the wizard.
2. Enter a unique name for the collection.
3. (Optional) Enter a description that will help you remember the profile content captured/restored by this collection.
4. Define the content you want to capture/restore with the collection by selecting rules in the Rules list. Use the plus-sign and minus-sign boxes to expand and collapse the tree structure to view all of the Applications, Desktop Settings, and File Rules.

To select a rule, check the corresponding check box; you can select any combination of the rules available in the Rules tree listing when defining a collection.

5. Click OK to save the collection and return to the Collection Manager dialog.

Note: When you delete a collection, the collection is removed from the core server. Any migration script referencing that collection will not run properly. You should also delete the script.

Migrating user accounts

In a scripted profile migration, all discovered local and domain user accounts on the source devices are captured by default (**Important:** Except for the All Users and Default User accounts).

All captured user accounts will be restored to the target devices. A user account that does not already exist on the target device will be created as a new local user account and its settings migrated. Before restoring user accounts, you can enter a default password for these new local user accounts. If a duplicate user account does already exist on the target device, the captured (source) user account's settings will be migrated to the existing user account, but the user's current password is preserved and should be used to log in.

Migrating application settings, templates, and associated files

Persistent application settings, template files, and associated files can be migrated as part of a device's profile. Application programs themselves are *not* migrated during profile migration (however they can be part of an OS image deployment). Each application's migration is defined by an application rule that can be added to a collection of rules.

Application rules are available for the following applications:

- **Microsoft Access**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.ade; *.adp; *.mad; *.maf; *.mag; *.mam; *.maq; *.mar; *.mas; *.mat; *.mav; *.maw; *.mda; *.mdb; *.mdbhtml; *.mde; *.mdt; *.mdz; *.mdw
- **Microsoft Excel**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.xls; *.csv; *.dqy; *.iqy; *.oqy; *.rqy; *.slk; *.xla; *.xlb; *.xlc; *.xld; *.xlk; *.xll; *.xlm; *.xls; *.xlhtml; *.xlv; *.xlw; *.dif; *.xlt; *.xlthtml
- **Microsoft Outlook**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.ics; *.msg; *.oft; *.pst; *.vcs; *.pab; *.rwz; *.oab; *.oft; *.srs
- **Microsoft PowerPoint**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.ppt; *.ppthtml; *.pps; *.ppa; *.pwz; *.ppz; *.pp1
- **Microsoft Word**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* *.doc; *.dohtml; *.gly; *.rtf; *.wbk; *.wiz
- **Microsoft Office Shared Components**
 - *Supported versions:* 95, 97, 2000, and XP
 - *Migrated files:* autocorrect lists (*.acl), custom dictionaries (*.dic), common toolbars, and all template files for supported Office applications, including: *.dot; *.dohtml; *.htm; *.pot; *.pothtml; *.xlt; *.xlthtml; *.mdn; *.mdz; *.wizhtml
- **Microsoft Internet Explorer**
 - *Supported versions:* 4.0, 5.0, 5.5, and 6.0
 - *Migrated files:* favorites (*.*), cookies (*.txt, *.dat), and ratings files (*.rat)

Current application support

Application rules are now available for the following applications:

- ACT!
- Adobe Acrobat
- Adobe Acrobat Reader
- Adobe Illustrator
- Adobe PageMaker

- Adobe Photoshop
- Lotus 1-2-3
- Lotus Approach
- Lotus FastSite
- Lotus Freelance
- Lotus Notes
- Lotus Organizer
- Lotus SmartCenter
- Lotus Word Pro
- MS ActiveSync
- MS FrontPage
- MS NetMeeting
- MS Outlook Express
- MS Visio
- Netscape
- Palm Desktop
- WinZip
- Yahoo Messenger

Application migration considerations

- Upgrade version migration is supported for Office 95 and 97 versions to Office 2000 or XP. For Office 2000 and Office XP, you can migrate applications to the same version.
- If an application is not installed on the target device, that application's settings and files will *not* be migrated, even if they were captured from the source device.
- Note that template files for all of the listed Microsoft applications are migrated as part of the Microsoft Office Shared Components rule. If you want to migrate template files, you must select Shared Components.
- To ensure a successful migration of all the most recent associated settings and files, close all applications before running a profile migration.

Additional application support

To obtain the latest application rule files offered by LANDesk, go to the official support Web site at <http://www.landesk.com/support/downloads/index.php>.

Migrating Desktop (PC) settings

Many of the customized and optimized settings on your devices can also be migrated. Each setting's migration is defined by a desktop rule that can be added to a collection of rules.

You can migrate the following desktop (PC) settings:

- Desktop shortcuts, files, folders, and briefcases

Note on briefcases: Remember to run Update All on a briefcase before migrating. Also, if your briefcase has links to files located in a "user-specific" directory that changes from one OS to another, and you migrate to a different OS, the files will be migrated but the links will be broken and need to be recreated.

- My Documents folder
- Mapped network drives

Note on duplicate drive letters: If there is a drive letter already mapped on the target device, that mapped drive is preserved rather than replaced, and the source device's drive letter mapping is not migrated.

- Printers (network)
- Wallpaper
- Screen resolution, color quality, and refresh rate

Note: Empty folders aren't captured.

Migrating files and folders

By creating your own customized file rules, you can migrate individual or multiple files determined by directory location and filename. File rules offer powerful control and flexibility by letting you:

- Create as many file rules as you want and add them to your collections.
- Include and/or exclude files by wildcard naming in a single file rule.
- Specify whether to include subdirectories.
- Redirect files to a new destination on the target device.
- Capture files from any fixed drive on the source device (including disk partitions), and successfully migrate the files even if the target device does not have the same partitioning.
- Retain the captured file's directory structure. If a captured file's associated directory structure does not exist on the target device, the path will be created and the file restored to it.

You can migrate files from a device's *fixed* drives, including disk partitions. Removable media, such as CD-ROM drives, and network shares are not supported. If the target device does not have a matching disk partition drive letter, a new directory named "Migrated_[drive letter]_Drive" is created at the root of the target device's C drive, and the files (along with their associated directory structure) are migrated to that new directory on the target device.

To create a file rule

Use the File Rules dialog to create new file rules or edit existing file rules. A file rule determines which files are migrated, based on the following criteria: drive and directory location; subdirectories; file naming including wildcard support, and destination location.

1. In the Collection Manager dialog, click **File rules** and then click **New** to open the File Rules dialog.
2. Enter a unique name for the file rule.
3. (Optional) Enter a description that will help you remember this file rule.
4. Specify all of the options on the dialog (for descriptions of the options, see About the File Rule dialog.)
5. Click **OK** to save the file rule and return to the Collection Manager dialog.

When you delete a file rule, the rule is removed from the core server. Any collection that contained that rule provides a notice about this change the next time you open or edit the collection.

Additional file migration considerations

- **Rules and collections:** You can create as many file rules as you like. You then add file rules to collections that may or may not contain other file, application settings, and desktop settings rules.
- **File path (directory structure):** The associated directory structure of a file is preserved by default.
- **Multiple controls in one file rule:** You can have any combination of multiple file inclusion and/or file exclusion controls in the same file rule.
- **File replacement handling:** The file captured from the source device replaces the existing file on the target device IF the captured file is newer than the Date Modified time stamp of the existing file.
- **File size limitation:** Because profile data is stored in sequential Windows cabinet (.CAB) files, which have a size limitation of 2 GB, you cannot migrate a single file that is 2 GB or larger. A file of that size is probably not common on devices, but you should be aware of this limitation.

Creating migration scripts with the OS Deployment/Migration Tasks wizard

The steps below outline the basic procedures for capturing and restoring a device's profile using the OS Deployment/Migration Tasks wizard. For more information about each of these steps, click the **Help** button located on each page of the script wizard.

Note: For capturing and restoring a profile with a user-initiated migration package, see the online help included with the LANDesk profile migration wizard.

To create a profile capture script

1. Click **Tools | Distribution | Manage scripts**.
2. In the Manage Scripts window, right-click **All OSD/profile migration Scripts** and then click **New OSD/profile migration script** in the shortcut menu to open the wizard. Or, in the Manage Scripts window, click the **New OSD/profile migration script** toolbar button.
3. Select **Capture profile**, and then click **Next**.
4. Enter a name and description for the profile capture script, and then click **Next**.
5. Select a pre-defined collection of rules (that determines the content of the profile), and then click **Next**.
6. Enter a UNC path and authentication credentials for the location where you want to store the profile data.
7. Click **Finish** to create the profile capture script and exit the wizard.

Using the Scheduled Tasks tool, you can now schedule the script to run on one or more target devices on your network.

Storing profile data for multiple devices (and multiple users)

Profile data is stored in Windows cabinet files (.CAB) in a directory structure located under the specified UNC path. If you run a profile capture script on multiple devices, each device's profile data is stored in a separate directory named after its unique Windows computer name. Likewise, if multiple users are discovered and captured on the same source device, each user's profile data is stored in a separate subdirectory (of the device's directory) named after the user login name. In other words, every migrated device has its own profile storage directory and contains a subdirectory for every captured user account on that device.

To create a profile restore script

1. Click **Tools | Distribution | Manage scripts**.
2. In the Manage Scripts window, right-click **All OSD/profile migration scripts** and then click **New OSD/profile migration script** in the shortcut menu to open the wizard. Or, in the Manage Scripts window, click the **New OSD/profile migration script** toolbar button.
3. Select **Restore profile**, and then click **Next**.
4. Enter a name and description for the profile restore script, and then click **Next**.
5. Enter the UNC path and authentication credentials to the location of the profile data you want to restore, and enter a default password for migrated new local user accounts (if left empty, the password is automatically set to "password").
6. Click **Finish** to create the profile restore script and exit the wizard.

Using Scheduled Tasks tool, you can now schedule the script to run on one or more target devices on your network.

Note: Windows 2000 SP3 and Windows XP are the only supported *target* Windows OSes.

Profile migration log file

Profile migration (both the scripted and user-initiated method) creates a "rolling" log file named PROFILEMIGRATION.LOG, that is saved in the user-specified profile data storage directory. Relevant information, such as time, specific operation, and status, are appended to the existing log file for each subsequent capture and restore operation. When the log file reaches 64 KB in size, it is renamed PROFILEMIGRATION.OLD and a new .LOG file is created. You can view this log file in any text editor.

Creating user-initiated profile migration packages

The User-Initiated Package dialog lets you create a self-extracting executable file that can be run on devices as a user-initiated profile migration.

User-initiated migration packages can be run on your devices, as well as computers that are not managed by LANDesk.

To create a user-initiated migration package

1. Access the Collection Manager dialog from the OS Deployment/Migration Tasks wizard, or by clicking **Scripts | Collection manager**.
2. Select **User-initiated packages**, and then click **New**.
3. Enter a unique name for the package. Do not type the filename extension here; the .EXE extension will be appended automatically to the name you enter.
4. Select a collection from the displayed list. The collection you select determines the profile content applications, desktop settings, and files. You can select only one collection per migration package.
5. To build the package, click **OK**. This may take some time, depending on the amount of profile content defined in the collection you selected.

The user-initiated migration package (.EXE) is saved by default to the following directory on your core server: c:\Program Files\LANDesk\ManagementSuite\LDLogon\PMScripts\Executables.

When you delete a user-initiated package, the package is removed from the core server. Other copies of the package may still exist depending on how and where you distributed the package to users.

Running user-initiated profile migration packages

You can distribute the user-initiated profile migration package to devices via e-mail or removable media and run it at the device, or you can store the package on a network share and run it from a device with access to that share.

The package launches a program called the LANDesk profile migration wizard that includes its own online help file. For more information, including step-by-step instructions for capturing and restoring a profile with user-initiated migration packages, click **Help** on any of the LANDesk profile migration wizard's pages.

Using the Web console

Overview

About the Web console

The Management Suite Web console enables IT professionals to automate systems management tasks and proactively control desktops, servers and mobile devices. From the Web console, you can:

- Remote control computers
- Run inventory queries
- View reports about computer inventory
- Schedule and deploy software packages to computers
- Monitor software license compliance

The Web console uses the infrastructure of your existing network to establish connections with the devices it manages. This greatly simplifies the job of managing your existing network, whether you manage a small network or a large enterprise environment.

The Web console runs on any Windows-based computer using these browsers, allowing you to manage your network resources even when you aren't at your desk.

- Internet Explorer 6.0 service pack 1 or later
- Mozilla 1.7 or later
- Firefox 1.0.0 or later

The Web console offers a subset of Management Suite's functionality from the convenience of a Web browser. The Management Suite console is your main resource for managing computers, but the Web console is useful when the management console isn't available. For more information, see "Chapter 6: Installing the Web console" in the *Installation and Deployment Guide*.

To run the Web console

1. From a networked computer, open a Web browser.
2. In the Address field at the top of the browser, enter the URL that will connect you to the site hosting the Web console pages. Normally, `http://<webservername>/remote`.
3. If a login dialog appears, enter your Windows username and password for the core you're connecting to and click **OK**.
4. Once you authenticate, links in the left navigation pane appear for the tasks you have rights to perform, such as creating queries, remote controlling clients, deploying software, and viewing reports.

If you don't know the URL to the Web console pages

Contact the person who installed the Web console, most likely the network administrator for your site.

If you can't see some of the left navigation pane links

It's because your network administrator is most likely using LANDesk Management Suite's role-based administration or feature-level security option that limits you to performing certain tasks that you have the rights to do. For more information about role-based administration and feature-level security, see "Chapter 6: Installing the Management Suite Web console" in the *Installation and Deployment Guide*.

The console

Starting the console

To start the console

1. On a remote workstation, open a browser and type the address of the console. This will be in the format of `http:\\corename\\remote`
2. Enter a valid user name and password.

If you're connecting to a remote core server, follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\\user name).

3. Click **OK**.

If the device list and buttons do not appear when you start the console, you may need to activate the core server.

About the Management Suite login dialog

Use this dialog to launch the console and connect to a core server.

- **Username**—Identifies a user. This might be an administrator user or some other type of product user with restricted access (for more information, see Role-based administration). The user must be a member of the Management Suite group on the core server. If you're connecting to a remote core server, enter the user name/domain.
- **Password**—The user's password.

Using the console

- My devices list
- Public groups
- Private groups

You can use tools to view, configure, manage, and protect the devices on your network—all from a single console. You can distribute and update software or configuration settings, diagnose hardware and software issues, use role-based administration to control users' access to features and devices, and use remote control features to train users or resolve problems. Additionally, if you are also using other LANDesk products, you can connect to them directly from the console. The Management Suite help is available at <http://www.LANDesk.com/Support/Downloads/>.

The top pane in the console displays the server you are logged in to and the user you are logged in as. The **My devices** list is the main window of the console and is the starting point for most functions. The left-hand pane shows available tools. The right-hand pane in the console displays dialogs and screens which allow you to manage devices and users, view reports, run discoveries, create and modify queries, and so on. You can resize the panes and columns of the **My devices** list. When no agents are installed on a device, the name and IP address are the only columns that contain information. In some instances, the operating system will also display.

Role-based administration

As a user, the devices you can view and manage in the **My devices** list and the management tools you can use are determined by the access rights and device scope assigned to you by the Administrator. For more information, see Role-based administration.

This section provides information about:

- My devices list
- Device icons
- Using shortcut menus
- Using tools
- Viewing device properties

My devices list

The **My devices** list contains the following groups and sub-groups. In addition, depending on your access rights and device scope, you can create your own groups for easier management of devices.

All devices

The **All devices** list shows the devices for the currently logged-in user, based on the user's scope, in a flat list (no sub-groups). When connected to a particular core server, the administrator can see every device managed by that core server. Product users, on the other hand, are restricted and can only see the devices that reside within their assigned scope (a scope is based on either a database query or a directory location).

Devices running product agents (Standard LANDesk agent and Inventory) automatically appear in the **All devices** list when they are scanned into the core database by the inventory scanner. Typically, this scan takes place for the first time during initial device configuration. Once a device is scanned into the core database it is considered to be a managed device—it can now be managed by that core server. For more information on setting up devices, see *Configuring client agents*.

Because the **All devices** group is populated automatically via an inventory scan, you may never need to manually discover devices. However, to discover devices not already in the core database (or to move unmanaged devices to the servers group), you can use the device discovery tool to scan the network for servers. For more information, see *Using discovery*.

The **All devices** group provides the following information for each device. Double-click **All devices** to open the list.

- **Name:** The device host name, such as the Windows* computer name.
- **IP address:** The IP address of the device.
- **Health:** The health and availability status of the device. This can be Normal, Warning, or Critical.
- **Agent:** The current agent running on the device.
- **Device type:** Displays the kind of hardware on the machine (AMT, IPMI, ASIC, or IPMI Advanced).
- **Operating system:** The type of operating system the device is running.
- **Up since:** The date and time the computer has been operating without interruption (in the time zone of the database).

When you select a device, the device's properties are displayed in the **Properties** pane below the device list. The **Properties** pane shows many important device attributes:

- **ID:** The identification number of the device. This number is determined by the sequence in which the device was added to the All devices list.
- **IP address:** The IP address of the device.
- **Manufacturer:** The device's manufacturer.
- **Model:** The model of the device.
- **Processor speed:** The speed of the device's CPU.
- **Processor type:** The type of the device's CPU.

From the console, you can remote control the machine, view a detailed inventory, assign attributes (such as Owner), and target the machine for an action, such as running a report. If the machine is a Linux server, you can use SSH and SFTP for remote access.

Double-clicking a device in the **All devices** list takes you to the , which contains device summary information, configuration, remote control options, and alert configuration information.

Public groups

The **Public groups** list shows groups of devices that have been created by a user with Administrator rights. They are visible to other users.

This list also shows blade chassis groups that are automatically created when a chassis management module (CMM) is added to the list of managed devices. The group lists the CMM and each associated blade server that you manage. You cannot edit a chassis group in the same way you edit a group you have created

Groups can be static or dynamic. Dynamic groups contain devices that meet predefined filter criteria, such as processor speed, server OS, or a custom attribute such as a device type. Static groups include a set list of devices, other static groups, or dynamic groups.





Private groups

The **Private groups** list shows groups of devices created by the currently logged-in user. Private groups are not visible to other users, so they can't be used by other users.

Device icons

Device icons display in the **All devices** list and show the current health status of each device. You can update the health status for servers one at a time as you select them in devices in the **My devices** list by clicking the **Refresh** toolbar button.

The following table lists the possible device and status icons and what they mean:

Icon	Description
	Server with Normal status
	Server with Warning status
	Server with Critical status
	Server with Unknown status

Using shortcut menus

Shortcut (context) menus are available for all items in the console, including groups, devices, queries, scheduled tasks, scripts, and so on. Shortcut menus provide quick access to an item's common tasks and critical information.

To view an item's shortcut menu, right-click the item. For example, when you right-click a managed device in the **My devices** list, its shortcut menu will typically display the following options:

- **Remove from group:** Removes the item from a user-defined group.
- **Target:** Moves the selected device to the Targeted devices list.
- **Ping device:** Verifies the server is awake.
- **Tracert device:** Sends a trace route command to view a network packet being sent and received and the amount of hops required for the packet to reach its destination.
- **Remote control:** Launches the remote control window, allowing direct access to the selected server from the console.

The help does not cover every console item's shortcut menu, but it is recommended that you right-click any item to see the options that are available.

Using tools

Tools are available through the left pane.

An administrator sees all of the tools in the left navigation pane. Other users will see only the tools (features) that are allowed by their assigned rights. For example, if a user doesn't have the Reports right, the Reports tool does not appear in the left navigation pane.

Here is a complete list of tools:

- **Device discovery:** Find devices on the network that aren't scanned into the core database.
- **Directory manager:** Lets you locate, access, and manage devices in other directories via LDAP (the Lightweight Directory Access Protocol).
- **Distribution:** Distribute software packages, use custom scripts, schedule distributions, and create software distribution tasks.
- **Queries:** Create and modify queries to the database to isolate specific devices that meet your criteria.
- **Remote control:** Remotely control devices and exchange files with them.
- **Reports:** Manage predefined service reports.
- **Scheduled tasks:** View all tasks (originating in Agent configuration, Vulnerabilities, Distribution, Device discovery, Scripts, or OS deployment) in the Scheduler.
- **Scripts:** Create and manage scripts.
- **Software licenses:** Provides the tools to implement complete, effective software asset management and license compliance policies.
- **Users:** Control user access to tools and devices based on user rights and scope.
- **Preferences:** Create custom inventory attributes and view licensing information.

When you click a tool name, the tool's window opens in the right pane.

Viewing device properties

In the **My devices** view, you can quickly view information about a device by clicking the device in the list and selecting **Properties** in the bottom pane.

More detailed information about the device is available in its inventory data. You can view inventory data in the **All devices** view by clicking the device and selecting the **View inventory** tab in the bottom pane to open the full **Inventory** window.

About the Properties screen

Use the Properties screen to view useful information about the selected server. The screen includes four buttons: **View details**, **View inventory**, **Assign attributes**, **Remote control**, **SSH**, and **SFTP**. Click each one to view related information.

View details

Click this button to open the summary of the local console. The local console allows you to view detailed information about the device. You can also view current alert settings and launch troubleshooting tools such as remote control.

View inventory

This button displays the full inventory of the selected server in a tree view.

Assign attributes

Assigns custom attributes, such as location or owner, to the selected device. These attributes must be created in advance in **Preferences**.

Remote control

Launches the remote control window, allowing direct access to the selected server from the console.

SSH

Provides secure access to the selected Linux server. If the selected server is not a Linux server, this option is dimmed.

SFTP

Provides secure FTP access to the selected Linux server. If the selected server is not a Linux server, this option is dimmed.

Targeting devices

The **Targeted devices** list enables you to complete numerous tasks on selected devices, such as deploying agents or distributing software to a select group of devices.

The recommended number of devices that you should add to the list is 250 or fewer. The devices will stay in the list until your console session times out (after 20 minutes of inactivity).

Add devices to the **Targeted devices** list by using **Find computer** at the top of the My devices, Device discovery, and Queries console pages. Search for one particular device, or search for several using the wildcard characters of % or *. Click the **Target** toolbar button to add the device to the **Targeted devices** list. If the button is not visible, click the << button.

If several devices are found, select the ones you want to add to the list, then click **Target**. If the returned device list spans multiple pages, you must click **Target computers** for each page. You can't select devices on multiple pages and click the buttons just once for all of the pages. You can click the down arrow below the toolbar on the far right to set how many devices you want to display per page. You can display up to 500 devices per page.

In either case, the targeted devices will appear in the **Targeted devices** list.

With one or more devices in the **Targeted devices** list, you can complete many actions on them, such as distributing software or deploying agent configurations to the targeted devices via the software distribution wizard. All the devices in the **Targeted devices** list will receive the software package, eliminating the need for a query.

To target devices


1. In the **My devices** list or the **Discovered devices** view, click the device you want to target for an action. You can select multiple devices by using the standard methods of multiple selection (SHIFT+click or CTRL+ click).
2. Click the **Target** button. If it is not visible, click << on the toolbar. The button is on the far right.

The selected devices are listed under the **Targeted devices** tab. Once they are listed under this tab, you can perform various actions on them, like add them to the database, reboot or turn them on and off, and so on.

Filtering the display list

The **My devices** list has a filter icon you can use to determine which devices appear in the list. You can filter by only one of the criteria (by device name or IP address), or you can combine the criteria to focus on a subset of computers.

To filter the display list

1. From the **My devices** list, double-click **All devices** or navigate to a group.
2. Click **Filter**  on the toolbar.
3. In the drop-down list, select **Device name** or **IP address**.
4. Set the parameters of the specified criteria by typing in the text box. In the **Find** box, the following extended characters are not supported: < , > , ' , " , !.

If you filter by device name, type the host name or range of computer names. You can enter wildcard characters to find certain computer names (such as *srv).

5. Click **Find**.

Using groups

You can organize computers in groups for easier management. You can create groups to organize devices based on function, geographic location, department, device attribute or any other category that meets your needs. For example, you could create a Web server group for all servers configured as Web servers, or create a group that includes all devices running a specific OS. You can right-click a group to open it, delete it, or target all of the devices it contains for actions such as software distribution, alert configuration, and inventory scanning.

The main **My devices** view contains the following groups:

- **All devices:** Lists all devices that can be seen by the currently logged-in user, based on the user's scope, in a flat list (no subgroups). For an administrator, **All devices** lists all devices that have been scanned or moved into the core database. Devices configured with the standard LANDesk agent automatically appear in the **All devices** group/folder when they are scanned into the core database by the inventory scanner. Users, including administrators, cannot create groups under **All devices**.
- **Public groups:** Lists groups/devices an administrator has added from the **All devices** group, as well as blade chassis groups. An administrator (a user with the LANDesk administrator right) sees all of the devices in this group, while other users see only the devices allowed by their scope. Only administrators can create groups under **Public groups**.
- **Private groups:** Lists groups/devices for the currently logged-in user, based on the user's scope. A user can create device subgroups only under **Private groups**. Users can add devices to their **Private groups** group, or any of its subgroups, by moving or copying them from the **Public groups** and **All devices** groups. All users can create groups under **Private groups**.

For more information on which servers you can view and manage in the device view, and the management tools you can use, see Role-based administration.

Group types

You can create and manage two types of groups:

- **Static groups.** A *static group* is composed of devices that you have added manually to that group. Static groups can only be changed by manually adding or removing devices.
- **Dynamic groups.** A *dynamic group* is composed of computers that meet filter or query definition. Each time the group is expanded, the query is resolved and the results are displayed. For example, a dynamic group may contain all devices currently in a Warning state. Machines would move in and out of the group as their statuses change.

To create a static group

1. In the console's device view, double-click the parent group (such as **Private groups**), and then click **Add group**.
2. Type a name for the new group.
3. Select **Static** and then click **OK**.

After you have created a static group, you can move/copy devices into the group by selecting them from the list and clicking **Move/copy** from the toolbar.

To create a dynamic group

1. In the console's device view, double-click the parent group (such as **Private groups**), and then click **Add group**.
2. Type a name for the new group.
3. Select **Dynamic** and then click **OK**.

After you have created a dynamic group, you must create a filter for it to determine which computers will appear in that group. You can specify a new filter or base the filter on an existing query.

To create a new filter

1. Select the dynamic group you created (this displays **Group properties** in the bottom pane).
2. From **Group properties**, select **Create a new filter** and click **Create filter**.
3. Select the filter criteria you want to use, then click **OK**.

To create a filter based on an existing query

1. Select the dynamic group you created (this displays **Group properties** in the bottom pane).
2. From **Group properties**, select **Create a filter based on an existing query**
3. Select the existing query you want to use to filter the group and click **New filter**.
4. Add any additional filter criteria you want to use, then click **OK**.

If you base a filter on an existing query and that query is later modified by you or another user, the filter based on that query will not dynamically change to match the modified query.

Custom columns

Use Custom columns to modify column names and fields. A Name is the name of the column, and a Field is the attribute(s) that can appear in the column (if the attribute is present). Any column changes you make will not be seen by other users. Custom column changes will be seen in the My devices view.

It is not advisable to create custom columns in which there can be multiple field names. For example, if you were to create a Computer.Software.Package.Name field and the server had multiple packages installed, Management Suite will list only one package name per line, even if the different package names are on the same device, making the All devices list and dashboard have multiple entries for the same device.

To change a column name

1. In the left navigation pane, click **Preferences**.
2. Click the **Custom columns** tab.
3. Click **Edit columns**.
4. In the top box, select a column heading and click **Add**.

The box shows a list that represents all of the inventory data currently in the database. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query. If you cannot find attributes you want to display, you can add them in the Custom attributes dialog. However, these attributes must be assigned to machines before they appear in the query dialog.

Note: If you're using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, and so on).

Note: If you select an attribute in the database that has a 1:* relationship, you will get duplicate entries for the device. Attributes with a 1:1 relationship (only one possible attribute, like Computer.System.Asset Tag), you will not receive duplicate entries.

5. To replace an existing heading, select the heading in the lower box, click **Edit**, make your modifications, and press **Enter**. The following extended characters are not supported: < , > , ' , " , !.
6. To change the order of the columns, select a column heading and click **Move Up** or **Move Down**.

Custom attributes

Attributes are characteristics or properties that belong to a device. The more attributes a device has in the database, the easier it becomes to uniquely identify the device. You can create custom attributes and assign those to a device or set of devices.

There are nine categories of non-inventoriable attributes to let you add custom data and associate it with specific devices. By explicitly listing the nine categories, this is modeled data, and now you can add that data as a custom column in the **My devices** view or run a query on that attribute.

The values you can add to that attribute however are dynamic and unlimited. For example, using the Location 1, 2 and 3 categories, you could enter values like assorted Country names in Location 1, Town names in Location 2, and Building names in Location 3. Then you could run a query to find a list of machines where Town name= London and you could then do something to that specific set of machines.

You must have the Administrator right to create custom attribute values.

To create custom attribute values

1. In the left navigation pane, click **Preferences**.
2. Click the **Custom attributes** tab.
3. Double-click the attribute name for which you want to create a custom value.
4. Type the new value in the **Attribute: name** box, and click **Add Value**.
5. To add another value, erase the value in the **Attribute: name** box, type the new value, and click **Add Value**.
6. To remove a value, select the value and click **Remove**.
7. To change the order the values will appear in the **Attribute: name** drop-down list, select the value and click **MoveUp** or **MoveDown**.
8. To replace a value, select an existing value, type the replacement value in the **Attribute: name** box, and click **Replace**.
9. When finished, click **OK**.

To assign custom attributes to devices

1. In the All devices list, click a device.
2. In the bottom pane, click the **Actions** tab.
3. Select **Assign attributes** from the left pane.
4. Each Attribute Name has a drop-down list of values. These values are created in Creating custom attributes above. Select a value from the drop-down list for the attribute name, and repeat as necessary.
5. Click **Targeted devices** or **Selected devices** to apply the attributes to those devices in the Target devices list or those selected and highlighted in the My devices list, and click **Assign**.

Page settings

Use **Page settings** to set display preferences for pages listing devices or displaying graphics.

1. In the left navigation pane, click **Preferences**.
2. Click the **Page settings** tab.
3. In the **Graph type** drop-down, select the type of graph you want to display in Reports.
4. In the **Items/page** box, type the maximum number of items you want to display in each page that uses pagination.
5. Click **Update**.

Role-based administration

About role-based administration

Use role-based administration to configure user access to product tools and other devices based on their administrative role in your system. With role-based administration, you assign scope to determine the devices a user can view and manage, and rights to determine the tasks they can perform.

Administrators (users with the LANDesk Administrator right) can access the role-based administration tools by clicking **Users** in the left navigation pane.

Role-based administration lets you assign product users special administrative roles based on their rights and scope. *Rights* determine the product tools and features a user can see and utilize. *Scope* determines the range of devices a user can see and manage.

You can create roles based on users' responsibilities, the management tasks you want them to be able to perform, and the devices you want them to be able to see, access, and manage. Access to devices can be restricted to a geographic location like a country, region, state, city or even a single office or department. Or, access can be restricted to a particular platform, processor type, or some other device hardware or software attribute. With role-based administration, it's completely up to you how many different roles you want to create, which users can act in those roles, and how big or small their scope of device access should be.

For example, you can have one or more users whose role is software distribution manager, another user who is responsible for remote control operations, a user who runs reports, and so on.

Example administrative roles

The table below lists some of the possible administrative roles you might want to implement, the common tasks that user would perform, and the rights that user would need in order to function effectively in that role.

Role	Tasks	Required rights
Administrator	Configure core servers, manage users, configure alerts, integrate other company products, etc. (Of course, administrators with full rights can perform any management tasks.)	Administrator (all rights implied)
Asset manager	Discover devices, configure devices, run the inventory scanner, enable inventory history tracking, etc.	Unmanaged device discovery, software distribution, and public query management
Deployment manager	Create images, deploy OS images, deploy PXE representatives, assign PXE holding queues, configure the PXE boot menu, create boot floppy disks, etc.	OS deployment
Helpdesk	Remotely control devices, chat, transfer files, execute software, shutdown, reboot, view agent and health status, etc.	Remote control, basic Web console
Application	Create software packages, scripts, and	Software distribution

manager	delivery methods, and distribute software packages.	and configuration
Reporting manager	Run predefined reports, print reports, etc.	Reports (required for all reports)
Software license monitoring manager	Configure applications to monitor, add licenses, upgrade and downgrade licenses, monitoring verify reports, etc.	Software license

These are just example roles. Role-based administration is flexible enough to let you create as many custom roles as you need. You can assign the same few rights to different users but restrict their access to a limited set of devices with a narrow scope. Even an administrator can be restricted by scope, essentially making them an administrator over a specific geographic region or type of managed device. How you take advantage of role-based administration depends on your network and staffing resources, as well as your particular needs.

To implement and enforce role-based administration, simply designate current local Windows users, or create and add new local Windows users, as Management Suite users, add the users to the LANDesk Management Suite user group, and then assign the necessary rights (to product features) and scope (to managed devices). Follow the procedures below:

Understanding rights

Rights provide access to specific tools and features. Users must have the necessary right (or rights) to perform corresponding tasks. For example, in order to remote control devices in their scope, a user must have the remote control right. Rights can be assigned to the user from either the Management Suite or Management Suite console, and are effective in both consoles.

When a right is not assigned to a user, tools associated with that right are not visible to that user in the product console. For example, if a user is not given the reports right, the reports item doesn't appear in the left navigation pane. The table below shows which rights are required for the tool to display for a user.

Tool	Rights needed to display in left navigation pane
My devices	Basic Web console
Agent configuration	Software distribution, Software distribution configuration, OS deployment
Alerting	Alerting/monitoring
Dashboard	Basic Web console
Device discovery	Discovery
Directory manager	Software distribution, Software distribution configuration, OS deployment
Distribution	Software distribution, Software distribution configuration, OS deployment
Monitoring	Alerting/monitoring
OS deployment	OS deployment
Queries	Basic Web console, Public queries, Reports
Reports	Reports, Software license monitoring, Patch, Patch compliance
Scheduled tasks	Discovery, Software distribution, Software distribution configuration, OS deployment, Patch, Patch compliance, Connection control manager
Scripts	Software distribution, Software distribution configuration, OS deployment, Patch, Patch compliance
Software assets	Software license monitoring
Users	Administrator

Vulnerabilities	Patch, Patch compliance
Preferences	Basic Web console

See the descriptions below to learn more about each product right and how rights can be used to create administrative roles.

Scope controls access to devices

When using the features allowed by these rights, users will always be limited by their scope (the devices they can see and manipulate).

LANDesk Administrator

The LANDesk Administrator right provides full access to all of the product tools (however, use of these tools is still limited to the devices included in the administrator's scope).

This is the default right for a newly added user, unless you've modified the settings for the Default Template User.

The LANDesk Administrator right provides users the ability to:

- See and access the **Users** tool in the left navigation pane
- See product licensing in **Preferences** in the left navigation pane.
- Perform all of the product tasks allowed by the other rights listed below

Note on rights and tools

The LANDesk Administrator right is exclusively associated with the **Users** tool. If a user does not have the LANDesk Administrator right, this tool will not appear in the console.

All of the tools in the product console are associated with a corresponding right (as described below).

Device discovery

The Device discovery right provides users the ability to:

- Find devices on the network that haven't submitted an inventory scan to the product core database through many ways, such as a network scan, Standard LANDesk agent discovery, and IPMI discovery
- Schedule periodic discoveries
- Move devices from Discovered to Managed

OS deployment

The OS deployment right provides users the ability to:

- See and access the **Scripts** tool in the left navigation pane
- Create and run OS deployment scripts
- Schedule OS deployment tasks
- Configure PXE representatives with the Deploy PXE Representative script
- Designate PXE holding queues
- Configure the PXE boot menu

Remote control

The remote control right provides users the ability to:

- Use the remote control options on a device's shortcut menu (otherwise, they are dimmed if the Basic Web console right is enabled)
- Remote control devices that have the remote control agent loaded
- Power up, shut down, and reboot devices (devices can only be powered up if they are IPMI devices)
- Chat with devices
- Execute device programs remotely
- Transfer files to and from devices

Software distribution

The software distribution right is a subset of the Software distribution configuration right, and provides users the ability to:

- Create and run software distribution scripts
- Ability to view and use the directory manager
- Schedule other script-based tasks

Public query management

The Public query management right provides users the ability to:

- Create queries available to all users
- Ability to create or delete public queries
- Ability to modify/edit existing public queries

Reports

The reports right provides users the ability to:

- See and access the **Reports** tool in the left navigation pane
- Run predefined reports

Patch manager

The Patch manager right is specific to the vulnerability scanning feature. For more information, see "Using the vulnerability scanner."

Asset configuration

The Asset configuration right is an administration-level right that is only available if you have purchased LANDesk Asset Manager. It provides users the ability to:

- See and access all the asset management links in the console: Assets, Contracts, Invoices, Projects, Global lists, Detail templates, and Reports.

- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

Asset data entry

The Asset data entry right is only available if you have purchased LANDesk Asset Manager, and provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global lists links in the console.
- Browse types and details (can't add, edit or delete them)
- Add items to the database by filling in data entry forms
- Edit items that have been added to the database

Software license monitoring

The software license monitoring right provides users the ability to:

- See and access the **Software licenses** tool in the left navigation pane
- Configure applications to monitor, add licenses, upgrade and downgrade licenses, and verify reports.

Software distribution configuration

The Software distribution configuration right is the primary distribution right. Users with this right can do everything available in software distribution.

- Create software packages
- Deploy packages to managed devices.

For more information, see "Software distribution."

Connection control manager

The Connection control manager right is a Management Suite right that provides users with the ability to:

- See and access the **Connection control configuration** tool in the Management Suite Tools menu and Toolbox
- Control the access to external devices to control and configure them

Patch compliance

The Patch compliance right provides users the ability to:

- Add and remove security definitions from the Compliance group
- Change the status of definitions contained in the Compliance group

Users with this right cannot edit custom definitions or security threat's custom variables.

Basic Web console

The Basic Web console right provides users with the ability to use the features associated with the right. The features are listed below, along with any exceptions within the feature.

- My devices (the right doesn't allow for the updating of public groups, or deleting devices under the Actions tab)
- Change preferences (but not custom attributes)
- Dashboard

Alerting and monitoring

The Alerting and monitoring right provides users with the ability to:

- Monitor the performance of various system and OS components, such as drives, processors, memory, processes, bytes/sec transferred by the system's Web server, and so forth
- Track the exact health of all managed devices
- Customize alerts to be sent by severity level (Critical, Warning, Informational, OK, Unknown) or threshold (for example, if the hard disk usage exceeds 90% of hard disk capacity)
- Choose the action to be taken if an alert exceeds a threshold (by adding information to the log, e-mailing a notice, running a program on the core or an individual device, or sending an SNMP trap to an SNMP management console on the network)

Adding product users

Product users are users who can log in to the product console and perform specific tasks for specific devices on the network.

Product users are not actually created in the console. Instead, users appear in the **Users** tab (in the left navigation pane, click **Users**) after they have been added to the LANDesk Management Suite group in the Windows NT users environment on the core server. The **Users** group shows all of the users currently residing in the LANDesk Management Suite group on the core server.

There are two default users in the **Users** group:

- **Default Template User**—This user is basically a template of user properties (rights and scope) that is used to configure new users when they are added to the LANDesk Management Suite group. In other words, when you add a user to that group in the Windows NT environment, the user inherits the rights and scope currently defined in the Default Template User properties. If the Default Template User has all rights selected and the Default All Machines Scope selected, any new user placed in the LANDesk Management Suite group will be added to the **Users** group with rights to all of the product tools and access to all devices.

You can change the property settings for the Default Template User by right-clicking it and clicking **Edit rights**. For example, if you want to add a large number of users at once, but do not want them to have access to all of the tools or devices, change the settings for the Default Template User first, then add the users to the LANDesk Management Suite group (see steps below).

The Default Template User cannot be removed.

- **Default Administrator**—This is the administrative user who was logged in to the server when LANDesk Software core was installed.

When you add a user to the LANDesk Management Suite group in NT, the user is automatically read into the **All Users** group in the **Users** window, inheriting the same rights and scope as the current Default Template User. The user's name, scope, and rights are displayed.

If you remove a user from the LANDesk Management Suite group in the Windows users environment, the user is no longer an active LANDesk user and can be deleted from the **Users** group. The user's account still exists on your server and can be added back to LANDesk Management Suite group at any time. Also, the user's subgroups under **User Devices**, **User Queries**, **User Reports**, and **User Scripts** are preserved so that you can restore the user without losing their data, and so that you can copy data to other users.

To refresh the **Users** list to display any newly added users, click **Users** and click the **Refresh** button on your browser.

To add a user or domain group to the LANDesk Management Suite group

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Groups | Groups** utility.
2. Right-click the **LANDesk Management Suite** group, and then click **Add to group**.
3. Click **Add**, then type or select a user (or users) from the list.
4. Click **Add**, and then **OK**.

Note: You can also add a user to the LANDesk Management Suite group by right-clicking the user account in the Users list, clicking **Properties | Member Of**, and then clicking **Add** to select the group and add the user.

If user accounts do not already exist in NT, you must first create them on the server.

To create a new user account

1. Navigate to the server's **Administrative Tools | Computer Management | Local Users and Group | Users** utility.
2. Right-click **Users**, and then click **New User**.
3. In the New User dialog, enter a name and password.
4. Specify password settings.
5. Click **Create**. The New User dialog remains open so that you can create additional users.
6. Click **Close** to exit the dialog.
7. Add the user to the LANDesk Management Suite group to have them appear in the Users group in the console.

You can now assign your product users rights and scope.

Creating scopes

A scope defines the devices that can be viewed and managed by a product user. Scopes can be assigned to the user from either the Management Suite or Management Suite console, and are effective in both consoles.

A scope can be as large or small as you want, encompassing all of the managed devices scanned into a core database, just a single device, or no devices. This flexibility, combined with modularized tool access, is what makes role-based administration such a versatile management feature.

Default scopes

Role-based administration includes two default scopes. These two predefined scopes can be useful when configuring the user properties of the default template user.

- **(Default) No Machines Scope:** Excludes all devices in the database.
- **(Default) All Machines Scope:** Includes all devices in the database.

You can't edit or remove the default scopes.

Custom scopes

There are three types of custom scopes you can create and assign to users:

- **Query-based:** Controls access to only those servers that match a custom query search. You can select an existing query, or create new queries from the **Assign devices to users** dialog, to define a scope. Note that you can also copy queries from the **Queries** groups in the network view directly into the **Scopes** group. For more information on creating queries, see "Creating database queries."
- **Group-based:** Controls access to only those devices located in the selected group. You can select groups from the **Group scope properties** dialog to define a scope.
- **LDAP- or custom directory-based:** Controls access to only those devices located in an Active Directory or NetWare eDirectory LDAP-compliant directory structure, or in a custom directory location. You can select directory locations when you click on the **New inventory scope** button.

You can assign more than one scope to any of the users. When multiple scopes are assigned to a user, the cumulative effective scope (i.e., the complete range of devices that can be accessed and managed as a result of the combination of assigned scopes) is a simple composite.

You can customize a user's effective scope by adding and removing scopes at any time. All types of scopes can be used together.

To create a scope

1. In the left navigation pane, click **Users**.
2. Click the **Scopes** tab, and then click the **New query scope**, the **New group scope**, or the **New inventory scope** toolbar button.
3. Enter a name for the new scope.
4. If you selected query-based, choose an existing query, or click **Define** to create a new query. Click **OK**.

5. If you selected group-based, choose a group, then click **OK**.
6. If you selected inventory-based, choose a directory, then click **OK**.
7. Click **OK** to save the scope and close the dialog.

Assigning rights and scope to users

Once you've added product users, learned about rights and how they control access to features and tools, and created device scopes to allow or restrict access to managed devices, the next step in establishing role-based administration is to assign the appropriate rights and a scope to each user.

You can modify a user's rights and scope at any time.

If you modify a user's rights or scope, those changes will take effect the next time that user logs into the console.

To assign rights and scope to a user

1. In the left navigation pane, click **Users**.
2. Select the **Users** tab to view all of the users that are currently a member of the LANDesk Management Suite group in the core server's Windows NT environment.

The **Users** tab displays a list of users, including their user name and assigned rights (a check character indicates the right is enabled or active).

3. Right-click a user, and then click **Edit rights**.
4. In the **User rights/scope** dialog, check or clear rights as desired.
5. Select a scope from the **Available scopes** list.
6. Click **OK**.

The new rights display next to the user's name in the list and will take effect the next time the user connects to the core server.

To delete a scope

1. In the left navigation pane, click **Users**.
2. In the **Scope** tab, click the scope you want to delete and click **Delete**. Click **OK**.

Exercise caution when deleting scopes. The users assigned to them will be able to access rights previously prohibited by the scope.

About the User rights/scopes dialog

Use this dialog to view and modify a user's assigned rights and scope. Open the dialog by selecting a user and clicking **Edit rights**.

- **Rights tab:** Lists the rights assigned to the user.
 - **LANDesk Administrator**
 - **Device discovery**
 - **OS deployment**
 - **Remote control**
 - **Software distribution**
 - **Public query management**
 - **Reports**
 - **Patch manager**
 - **Asset configuration**

- **Asset data entry**
- **Software license monitoring**
- **Software distribution configuration**
- **Connection control manager**
- **Patch compliance**
- **Basic Web console**
- **Alerting and monitoring**
- **Scope tab:** Lists the scopes assigned to the user.
 - **Assigned scopes:** Identifies the user's current scopes.
 - **Add:** Opens the **Add scope** dialog where you can select a scope to add to the user.
 - **Remove:** Deletes the selected scope.
 - **Apply:** Saves your changes to the user's properties and closes the dialog.
 - **Cancel:** Closes the dialog without saving changes.

Remote server access

About remote access

Use the remote control feature to easily resolve device problems from one location. Read this chapter to learn about:

- Remote controlling devices
- Using remote control
- Configuring Windows 2003 client security for remote control
- Accessing remote Linux servers

Remote controlling devices

Remote control allows users to remotely diagnosis and troubleshoot many device problems. During a remote session, you can do anything at the remote computer that a user sitting at it could do while using the keyboard layout of your machine, not that of the target machine. All of your actions happen in real time on that computer. You can set remote control access through the Role-based administration tool. It allows you to:

- Fix software and hardware problems quickly by allowing authorized users to check and take control of a computer remotely
- Access remote files
- Transfer files in either direction
- Execute remote applications
- Remote reboot

Using remote control

To use remote control from the console, you must first install the remote control viewer. You need administrative privileges on the local computer to install the viewer, which you are prompted to download the first time you access the remote control page. If necessary, you can uninstall the remote control viewer using the Windows Control Panel's Add/Remove Programs applet. Look for **LANDesk Management Suite Remote Control Console** in the program list. The remote control agent also must be installed on each remote device you want to control.

To remote control a device

1. In the dashboard, right-click the icon of the device you wish to connect to and select **Remote control**, which will launch the viewer.

or

In the console, right-click the device you wish to connect to and select **Remote control**, which will launch the viewer.

2. In the Administrative console, single-click the device and select the **Remote control**, **SSH**, or **SFTP** button in the **Properties** tab in the lower pane

or

Double-click to launch the local console and click **Remote session** in the left navigation pane.

You can also remote control more than one computer at a time. After starting one session, return to the dashboard or console and select another computer.

To be remote-controlled, Windows servers must have the LANDesk remote control agent installed and loaded. This agent is installed by

- Creating an agent configuration task in the console and scheduling a deployment to the device, or
- Mapping a drive from the device to the core server and running the appropriate agent configuration.

This agent may be loaded as a resident service in order to provide immediate access to the machine, or it may be installed as an on-demand agent that loads only when needed.

Additionally, you can install the remote control mirror driver to improve the performance of detecting, capturing, and compressing screen changes if the server CPU is slower (< 2.0GHz) or the network is fast (> 100mpbs). Note that remote control doesn't support DOS graphics or full-screen DOS windows. The command prompt window may not display initially when using the mirror driver. If this occurs, minimize the window then maximize it.

To access a Linux device remotely, at least the standard LANDesk agent must have been deployed to that device. After clicking that device in the **My devices** list, you have a choice of SSH and SFTP on the lower pane. Select either option to launch a new window. Note that if the device has not had any agent deployed yet, double-clicking that device in the **My devices** list and selecting **Remote session** will launch the Windows viewer as a default behavior, as the OS is not yet known. The viewer will report that it was unable to connect to the client.

Configuring Windows 2003 client security for remote control

The resident service uses Windows NT security. To work with Windows 2003 servers, you must configure the server clients so that the Windows 2003 sharing and security model for local accounts is classic (local users authenticate as themselves). If you don't do this, the default guest-only authentication won't work with remote control's Windows NT security.

To set the Windows 2003 security model to classic

1. On the Windows 2003 client, click **Start | Control Panel**.
 2. In the **Administrative Tools, Local Security Policy** applet, click **Security Options > Network access: Sharing and security model for local accounts**, and set it to **Classic - local users authenticate as themselves**.
-

Controlling remote Windows devices

To start remote control

1. In the administrative console's **All devices** group, or from within one of your groups, click the device you want to control.
 2. Select **Remote control** in the **Properties** tab in the lower pane to launch the viewer.
- Or
3. Double-click the device you want to control and click **Remote session** in the left pane.

Once you've taken control of a remote device, its screen appears in the **Viewer** window with Autoscroll enabled. If the remote control agent is loaded, the **Session messages** window in the viewer tells you that the agent is found and what protocol it's using.

To use hot keys

1. You must be actively remote controlling a device to use hot keys.
2. With the focus on the **Viewer** window, press the hot key combination for any one of the available actions.

The available hot keys are found in the **Special key** icon on the toolbar. You may also change the default mappings.

About the Viewer window focus

If you find that the hot keys don't work, the focus isn't on the **Viewer** window. If the border is blue/black, the focus isn't on the window. Click inside the window to change the border to yellow/black. You should now be able to use hot keys.

To view different areas of a remote device screen

By default the Autoscroll option is enabled. When enabled and currently remote controlling a device, you can place your cursor along the yellow/black border of the **Viewer** window and scroll up, down, or side to side. The closer your cursor gets to the border, the faster the scrolling will occur. If you wish, you can disable Autoscroll in the **Options** menu. You can then use the **Move remote screen** icon. Your cursor will become a hand that you can click, drag, and release to view various areas of the remote screen.

Viewing connection messages

You can use the **Viewer** window's connection messages section to view a history of status messages sent to the status bar (such as remote control agent package exchanges). In addition to the other information this history contains, it lets you:

- Diagnose problems with the session
- Check whether the remote control agent is loaded
- Check the status of the remote control agent

To view connection messages from the console

1. In the **Viewer** window, click **View**, and click **Connection messages**.

Saving connection messages

While you're in a remote control session, you have the option of saving the connection messages. These messages may be useful as an audit trail or if you need to troubleshoot any issues related to using remote control on a particular device.

To save connection messages

1. In the **Viewer** window, click **File**, and click **Save connection messages**.
2. In the **Save As** dialog, type in a file name and save as a .TXT file. The connection messages are saved to the My Documents folder by default.

If the remote control agent is loaded, the **Session messages** window tells you that the agent is found and what protocol it's using. You will also see a magnifying glass icon appear on the server you selected.

Executing programs remotely

In the **Viewer** window, you can start any program on a remote device to diagnose issues.

To execute programs remotely

1. In the toolbar's **Run** field, enter the path for the program you want to run. If you need to browse the program, click the drop-down list and select **Browse**.
2. To run the program on the remote device, click the **Remote execute** icon to the left of the **Run** field.

Transferring files to remote devices

You can use the remote control **Viewer** window to transfer files to and from your machine and the remote device. In essence, this works as though you've mapped a drive to the remote device. You can only transfer files to/from devices that have the remote control agent installed. This feature works even if you're not currently remote controlling a device as long as the connection has been created. The **Run each Explorer window in a separate process** option doesn't work with file transfer.

To transfer files to a device

1. Click **Tools | File transfer**. Windows Explorer appears.
2. Select a file to transfer by clicking the filename. Right-click the file and select **Copy**, or select to drag and drop.
3. Scroll down the Windows Explorer tree to **Remote Computers**. Below this you should see the name of the remote device you're controlling. Select a folder to paste the file to, then right-click and select **Paste**.

Similarly, you can also transfer files from a remote device to your device.

Shutting down and rebooting remote devices

You can remotely shut down or reboot devices. When you do, a message box appears on the remote device with a warning that the system will shut down in 10 seconds. If someone is currently at that machine they can click a **Shutdown** or **Cancel** button. If no action is taken the reboot will happen when the countdown reaches 0. When typing a time before rebooting the device, the maximum number of seconds allowed is 300 seconds (five minutes).

If the device has applications open with unsaved data, those applications will probably interrupt the shutdown when they prompt for the user to save. You may have to remote control the device and save/close applications for the shut down or reboot to work.

Configuring session options

Use items under the **Options** menu to enhance the quality of a remote control session. You can speed up the viewing rate and change the **Viewer** window settings.

In the **Change settings** tab:

- **Autoscroll:** Set by default. Enables the **Viewer** window to scroll as you move the cursor closer to the window border. Toggle on/off; item is on when a check mark appears next to it.
- **Keyboard and mouse lockout:** Locks the server's keyboard and mouse so that only the user running the **Viewer** window can control the remote server. Toggle on/off; item is on when a check mark appears next to it. Note that special key combinations in Windows such as "CTRL-ALT-DEL" or the "Windows Key+L" aren't locked out.
- **Synchronize clipboards:** Set by default. Synchronizes the keyboards between the **Viewer** console and the remote server so you can paste information between the two machines. Toggle on/off; item is on when a check mark appears next to it.
- **Blank server screen:** Blanks the server's screen so only the user running the viewer can see the user interface display on the remote server. Toggle on/off; item is on when a check mark appears next to it.

In the **Optimize performance** tab:

Optimize performance for: Select Modem, Broadband, LAN, or custom as appropriate for your network environment

Display:

- **Use the mirror driver:** Loads the mirror driver for enhanced performance on slower machines. Toggle on/off; item is on when a check mark appears next to it.
- **Suppress the wallpaper:** Speeds up the viewing rate by suppressing the remote device's background wallpaper. Ornate wallpapers can substantially slow down a remote control session. Toggle on/off; item is on when a check mark appears next to it.
- **Color depth reduction:** If you're connecting via a slow link or Dial-up Networking connection, this option reduces the amount of transferred color information. The closer you move the slider to full reduction, the more color artifacting you might see.

Mirror driver

During the Management Suite installation, you had the option to install the remote control mirror driver. This driver can reduce the amount of time required to see the target machine's desktop and increase the visual quality of the targeted desktop's image. A raster-based approach to screen capture can be implemented without any drivers, which is a huge advantage if the agent is to be downloaded over the Internet or installed on machines by users who do not have administrative rights. However, significant performance improvements can be achieved by using a driver that receives all of the output that Windows is sending to the real display driver.

Accessing remote Linux devices

To access a Linux server remotely, at least the standard LANDesk agent must have been deployed to that server. After clicking that Linux device in the **My devices** list, you have a choice of **SSH** and **SFTP** in the lower pane. Selecting either option will launch a new window.

Note that if the server has not had any agent deployed yet, double-clicking that device in the **My devices** list and selecting **Remote session** will launch the Windows viewer as a default behavior, as the OS is not yet known. The viewer will report that it was unable to connect to the client.

If you select SSH access, a window opens with an SSH session on the remote server. You must provide a username and password to access the server. When you have authenticated, a secure shell session opens on the remote server.

If you select SFTP access, a window opens with a secure FTP view of the remote server (based on an SSH connection). You must provide a username and password to access the server. When you have authenticated, you can use the secure FTP functionality to transfer files between your computer and the remote server.

Software distribution

Software distribution overview

The Software distribution tool gives you the ability to distribute software packages to target devices. The tool supports many different types of packages. Software distribution consists of these main steps:

1. **Create or obtain a software package.** The software package can be one or more MSI files, an executable, a batch file, RPM files (Linux), or a package created with LANDesk's package builder. If the software package is a batch file, see "Using the Start command in a batch file package" below. In most cases, the software package needs to contain everything necessary to install the application you're distributing. Put the package on your delivery server.
2. **Create a distribution package.** The distribution package contains the files and settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, command-line switches, and so on. These settings are stored in the database and create a "distribution package." Once you create a distribution package, the information is stored in the database and can easily be used in multiple tasks.
3. **Create a push delivery method.** The push delivery method defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Don't create a delivery method every time you want to distribute a package. Delivery methods allow you to define best practices for deploying software. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.
4. **Schedule the distribution job in the Scheduled tasks window.** Here you specify the distribution package, the delivery method, the devices that need to receive the distribution package, and when the task should run.

When the scheduled time occurs, the scheduler service will start the scheduled task handler which contacts the software distribution agent on each device and informs it that the package is ready for installation.

The software distribution agent then obtains the package from the delivery server and processes it on the device by installing or removing the packaged files.

After the package is processed, the software distribution agent sends the result to the core server, where it's recorded in the core database.

Separating distribution tasks into two parts, distribution packages and delivery methods, simplifies the distribution process. Now you can create delivery method templates that are independent of a particular package. If you have different people in your organization that create packages and distribute packages, these changes help simplify job roles and task divisions. Package creators can now work independently from package deliverers.

Software distribution enables you to deploy software and file packages to devices running the following operating systems:

- Windows 2000
- Windows 2003
- Windows XP
- Red Hat Enterprise 3 Linux AS and ES
- SUSE LINUX Server 9 (Advanced, Enterprise, and Professional)

Devices receiving the software distribution packages must have the following LANDesk agents installed:

- Standard LANDesk agent
- Software distribution agent (Windows only)

Software distribution features include:

- Delivery methods enable detailed control over how tasks complete
- Easy task scheduler integrates with the inventory database to make target selection easy
- Real-time status reporting for each deployment task
- Full-featured package builder to build complete software packages
- Ability to distribute any package type, including MSI, setup.exe, and other installers

If you don't have an existing package that you want to deploy, you can use LANDesk's package-building technology to create a standalone executable program for the required software installation. A Web server or network server can be configured as a "delivery server" to store distribution packages. Through the console, you can schedule the distribution task. The core server communicates the package's location (URL or UNC path) to the device, and the device then copies only the files or the portions of the files it needs from the delivery server.

For example, if you're reinstalling a previously deployed software program because some of its files were corrupted or missing, the system copies only the damaged or missing files, not the entire program. This technology also works well over WAN links. You can store the package on multiple servers, and then schedule devices to use the server appropriate to their needs (that is, location proximity, bandwidth availability, and so on).

Using the Start command in a batch file package

The batch file distribution package has been designed to run as if it were issued from the Run command in the Windows Start Menu. When a batch file is executed using the Run command, it closes upon completion. A program that is required to run in an open command window will close prematurely when run through a batch file distribution package.

The program can be configured to continue running by using the "Start" command in the batch file. The "Start" command will actually spawn a new command window that remains open after the batch file has completed and closed the initial command window.

Here is an example of a batch file that uses the "start" command to spawn a new command window running the Sample.exe program.

```
start "Title" /D "c:\program  
files\ManagementSuite\ldclient\sdmcache\swd\alertttest" Sample.exe
```

The first parameter ("Title") is the name of the command window that will be displayed in the title bar. Note that the title is mandatory because the path to the executable will be misinterpreted as the Title if it is omitted. If the path to the executable includes a space, it must be in quotes. If the title were not present, the quoted path to the file would be mistaken for the title, even though the /D switch indicating the path is present.

This single line batch file runs Sample.exe in a new command window titled "Title." For more help on the Start command, type the command with either the /h or /? switch at a command prompt.

Setting up a distribution package delivery server

The delivery server is the server that stores the software distribution packages. It can be either a Web server or a Windows NT/2000/2003 server. We recommend that for best results the packages be URL-based. In general, properly configuring a URL is less work than configuring a UNC path.

Delivery server Requirements

Web server	Microsoft Internet Information Server 5.0 or higher running on Windows NT or Windows 2000/2003, or any HTTP 1.1 compliant Web server with byte range support.
Network server	Windows NT 4.0 or Windows 2000/2003

Configuring Windows Web servers for software distribution

To configure a Microsoft IIS 5.0 Web server for software distribution

These steps explain how to create a virtual directory on a Web server and enable it for browsing. In general, virtual directories need to allow reading and directory browsing and anonymous access to the virtual directory must be enabled. Execute must not be set or the share won't work correctly. You also may want to disable write permissions so devices can't change the directory's contents.

1. Create a directory on the Web server where you want to store your software distribution packages. The usual location for such a directory on an IIS Web server is a subdirectory in the c:\inetpub\wwwroot directory.
2. Copy the packages to this directory.
3. From the **Control Panel**, double-click **Administrative Tools** and then **Internet Services Manager**.
4. In the right panel, double-click the icon with the device's name and then click **Default Web Site**.
5. In an empty area in the right panel, right-click and select **New**, then click **Virtual Directory**.
6. From the wizard, click **Next** and then enter an alias for your directory. Click **Next**.
7. Either enter the path or browse to a path and click **Next**.
8. In the **Access Permissions** dialog, enable **Run script** and **Browse**. This enables you to browse packages when creating the software distribution script. Click **Next** and **Finish**.
9. To enable **Port 80** on the Web server, in the left panel, right-click **Default Web Site**.
10. Click **Properties**. In the **Web Site Identification** dialog, the **TCP Port** box should display 80. If it doesn't, click **Advanced** to add the port.
11. Ensure that the Web site is available by opening a browser and entering the URL for your Web server and virtual directory. For example, if the name of your Web server is Test and the name of the virtual directory is Packages, enter the following URL:

`http://Test/Packages`

A list of the packages you have copied to this directory should appear.

The size and number of packages you put in this directory is limited only by available disk space. Subdirectories can be created to logically group packages. Each subdirectory that's created must have the above access permissions set.

Once you copy the packages to a package share on a Web server, they're staged and ready to be copied to the target devices. When scheduled, the URL or UNC path of the package is passed to SDCLIENT.EXE (the device agent) as a command-line parameter. SDCLIENT.EXE manages the file transfer, starts the installation, and reports the status. Although the HTTP protocol is used for the file transfer, the status report is returned through the standard LANDesk agent.

The Web server communicates with the device to ensure that the package copies correctly. If the package transmission is interrupted during the download, the Web server can use the HTTP protocol to restart the download at the point where it stopped. The Web server doesn't check, however, to ensure that the package was installed correctly. That traffic is TCP-based, and it returns the status to the core server using the standard LANDesk agent.

To configure a Microsoft IIS 6.0 server for software distribution

Windows 2003 Server handles virtual directories differently than Windows 2000. On a Windows 2003 server, if you select a directory and from its shortcut menu make it a Web share, the directory registers itself in IIS 6 as a Web application rather than a virtual directory. The problem is that as a Web application, when an executable file is selected, the Web server attempts to run the file as a Web application rather than download the file to the user. The resolution is to go into IIS, change the shared directory from a Web application to a virtual directory, and turn off execute permissions.

Linux packages information

When hosting RPM files for Linux on a Windows server, files without a registered MIME file type will fail to execute unless you do the following.

To register MIME file types

1. Launch Internet Information Services (IIS) Manager.
2. Expand the local computer in the tree.
3. Click **Web Sites > Default Web Site**.
4. From the package Web share's shortcut menu, click **Properties**.
5. Click the **HTTP Headers** tab.
6. Click **File Types** on the **MIME Map** section.
7. Click **New**.
8. In the **Associated Extension** box, type **.RPM**.
9. In the **Content Type (MIME)** box, enter **text/plain**.
10. Click **OK** twice and apply the changes.

Configuring a network server for software distribution

Devices that don't have a browser must receive distribution packages from a UNC path on a Windows NT/2000/2003 network server. This can be the same folder as the one you set up on your Web server. For UNC path-based distributions to work correctly, you must enable a null-session share folder on your network server. Use the SYSSHRS.EXE utility to create a null-session share folder.

1. To set up a shared folder on your network server, right-click the folder you want to share and then click **Sharing**.

2. Click **Share this folder** and click **Permissions**.
3. Add the appropriate file rights such that
 - **Core (Task Scheduler user):** Access at deployment time (when the package is deployed).
 - **Console (Logged-in user):** Access while creating the package to browse for a file or check SWD packages and MSI packages to verify they contain unique IDs.
 - **Target (null session):** Uses a null-session share to read the package.

One simple method to accomplish this is to give the Everyone group and the Guest and Anonymous accounts read rights.

4. The Everyone group needs file access rights to the files within the share. To do this, click **Security**, click the **Everyone** group, and click **Read & Execute, List Folder Contents, and Read permissions**.
5. From your network server, click **Start | Run** and browse to the LDMAIN\Utilities folder on your core server.
6. Run the **SYSSHRS.EXE** utility.

Note: Although this utility states that it's for Windows NT devices, it also works on Windows 2000/2003 devices.

7. Check the shared folder you set up and click **Apply** and then **Close**.
8. Copy the software distribution packages to this folder on the network server.

Additional steps needed to configure a Windows Server 2003:

9. Open the Group Policy Object Editor by clicking **Start | Run**, and typing "gpedit.msc". Right-click **Network access: Let everyone permissions apply to anonymous users**, click **Properties**, and select **Enable**.
10. In the Group Policy Object Editor, right-click **Network access: Restrict anonymous access to Named Pipes and Shares**, click **Properties**, and select **Disable**. The policy just below it must contain the name of the share that is to be the null session share.

The size and number of packages you store on the network server is limited only by the available disk space.

For more information about the SYSSHRS.EXE utility, download the SHARES.EXE package from <http://www.LANDesk.com/support/downloads/Resource.aspx?pvid=12&rtid=10> and extract the documentation.

Distributing software to Linux devices

Once you've deployed the Linux agents, you can distribute software to your Linux devices. The initial Linux agent deployment uses an SSH connection. Once the agents are installed, the core server uses the standard LANDesk agent to communicate with the Linux server and transfer files. To distribute software to a Linux device, you must have Administrator rights.

You can only distribute RPMs to Linux devices. The Linux agents will automatically install the RPM you distribute. The RPM itself isn't stored on the server after installation. You can install and uninstall the RPM you specify using software distribution. You can only use push delivery methods with Linux software distribution. For Linux software distribution, the settings in the push delivery method are ignored, so it doesn't matter which push delivery method you select or what the settings in it are.

The distribution follows this process:

1. The core server connects to the Linux device through the Standard LANDesk agent
2. The device downloads the package
3. The device runs a shell script that uses RPM commands to install the RPM package
4. The device sends status back to the core server.

You can store Linux RPMs on HTTP shares. Linux software distribution doesn't support UNC file shares. For HTTP shares, make sure you've enabled directory browsing for that share. If you use an HTTP share on a Windows device other than the core, you need to configure IIS with the correct MIME type for RPM files. Otherwise, the default MIME type IIS uses will cause the RPM to fail to download the file.

To configure the RPM MIME type on Windows devices

1. From Windows **Control Panel**, open **Internet Services Manager**.
2. Navigate to the folder that hosts your distribution files. From that folder's shortcut menu, click **Properties**.
3. On the **HTTP Headers** tab, click the **File Types** button.
4. Click **New Type**.
5. For the **Associated Extension**, type **rpm**. Note that rpm is lower-case.
6. For the **Content type**, type **text/plain**.
7. Click **OK** to exit the dialogs.

Once you've hosted the files on your package share, create a new Linux distribution package, associate it with the delivery method you want, and schedule the delivery.

Distribution file descriptions

This is a list of the files used in SWD, as well as descriptions of how they work together. You can use this information to customize how packages are created, stored, and deployed in your organization.

These files are installed at the core server:

- ManagementSuite\CUSTJOB.EXE
- ManagementSuite\SDMAKINI.DLL
- ManagementSuite\LANDesk.ManagementSuite.WinConsole.dll
- ManagementSuite\INSTALL\EN_PKG_BLD\SETUP.EXE
- ManagementSuite\LDLOGON\SDCLNSTL.EXE

These files are installed at the device:

- C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE
- sdistexh.dll
- sdistmsi.dll
- ldapinfo.dll
- C:\Program Files\LANDesk\LDClient\AICLIENT.DLL
- C:\Program Files\LANDesk\LDClient\SDMCACHE (this is an empty folder)
- C:\LDCLIENT.LOG (this file is created by the SDCLIENT.EXE file)
- INST32.EXE
- EUNINST32.DLL (or other locale-specific resource file)
- %WINDIR%\aiclient.log
- %WINDIR%\inst32.log
- %DEST%\WebPortal\WebPortal.exe
- %DEST%\WebPortal\SDClientMonitor.exe
- %DEST%\WebPortal\style.css
- %DEST%\WebPortal\img\LANDesk_logo.jpg
- %DEST%\WebPortal\img\logo.jpg
- %DEST%\WebPortal\img\SWDPortalTitle.jpg
- %DEST%\WebPortal\img\titlerl.gif
- ldredirect.dll
- sdcln.dll
- sdmsi.dll

File descriptions

SETUP.EXE: This standalone, binary installation file is used to create package-building computers, placing the Package Builder, Package Builder wizard tools, and accompanying online help files onto the computer. Each application that you package with Package Builder is made into a self-extracting .EXE.

If you're using the Web Console, you must copy the .EXE to the packages folder on your Web server for users to access.

SETUP.EXE installs the following types of files on the package-building computer in the Program Files\Intel\Package Builder folder:

- BUILDER.EXE: Enhanced Package Builder executable

- **ENUBLDR.DLL:** Enhance Package Builder resource file
- **REPLICATOR.EXE:** Package Builder wizard executable
- **ENUREPLC.DLL:** Package Builder wizard resource file
- **BASIC.CFG:** A simple installation script for building a software distribution package
- **TYPICAL.CFG:** A more complex installation script for building a software distribution package
- **ENUBLDR.HLP:** Help file for the Package Builder
- **ENUBLDRI.HLP:** Help file for the Package Builder wizard

CUSTJOB.EXE: This file is launched directly by the scheduler when a job is to begin.

SDC_INSTALL.INI: This job script is processed by CUSTJOB.EXE. It copies SDCINSTL.EXE to a remote device and then executes it on that device via the standard LANDesk agent (CBA). This file is placed in the DTM\Scripts folder.

SDCLNSTL.EXE: This file installs the SWD client files SDCLIENT.EXE and AIClient.DLL on Windows 95/98 and Windows NT/2000/2003/XP devices. This file is placed in the DTM\LDLogon folder on the core server.

SDCLIENT.EXE: This file is ultimately placed on the device in the C:\Program Files\LANDesk\LDClient folder. It's invoked with command-line parameters that include the URL or UNC path of the distribution package to be installed. This invocation is normally a result of the core server Scheduler calling CUSTJOB.EXE.

SDISTEXH.DLL: Handles the installation and removal of packages built by the LDMS 6.3 and earlier package builder.

SDISTMSI.DLL: Installation/removal library for Microsoft Installer (MSI) packages.

AIClient.DLL: This file is called by SDCLIENT.EXE; it's copied to the same folder as SDCLIENT.EXE.

INST32.EXE: This is the actual installer program. It's embedded within every self-extracting package. It's also installed into the LDClient folder and launched by SDCLIENT.EXE whenever a request to install a software package is received.

ENUINST32.DLL: This is a locale-specific resource file, and its name varies with the locale.

AIClient.LOG: This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to AIClient.LOG1. When the new AIClient.LOG file exceeds the 50 KB limit, AIClient.LOG1 is renamed to AIClient.LOG2. It's incremented one more time to AIClient.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current AIClient.LOG file.

INST32.LOG: This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to INST32.LOG1. When the new INST32.LOG file exceeds the 50 KB limit, INST32.LOG1 is renamed to INST32.LOG2. It's incremented one more time to INST32.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current INST32.LOG file.

WEBPORTAL.EXE: This CGI-based portal communicates through the local client's Standard LANDesk agent and checks with the local software distribution cache for policies that apply to the local device/user. The portal then displays a Web page listing available policies. All the files in the WebPortal folder pertain to this application.

REDIRECT.DLL: Aids in the support of redirecting file download to a specified preferred package server.

About Distribution packages

The **Distribution packages** view shows the available distribution types and any packages you've created for each distribution type. When you select a distribution package you've created, you can view the properties for it, delete it, clone it, or reset the package hash.

To create a new distribution package, select a distribution package type in the toolbar and click **New**.

For more information on software distribution, see "Software distribution overview." For more information on the distribution package dialog options, see "Distribution packages and delivery methods dialog help."

Understanding the distribution package types

Software distribution supports these package types:

MSI

These are packages in the Windows Installer format. You must use a third-party tool to create MSI packages. These packages consist of a primary .MSI file and can include supporting files and transforms. Transforms customize how MSI packages are installed. If your MSI package consists of multiple files, make sure you add all of them as additional files in the Distribution package dialog.

Software distribution packages (SWD)

These are packages built with the Management Suite Package Builder (installed separately).

Executables and batch files

These types of packages will run if the command was issued from a DOS prompt. Add command line options in the Distribution packages dialog.

Linux

The product supports Red Hat Linux ES and AS, and SUSE Linux Server 9 (Enterprise, Professional, and Advanced). RPM deployment is supported. Scripting is not supported. Additional files need to be in a location where Linux can reach them. A Web share or an anonymous HTTP site can be used to store RPMs. Linux does not support mapped drives.

Package Groups

My packages: Packages that the current user has created. The administrative users can also see these packages.

Public packages: Packages that users have marked common. Anyone who schedules a package from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.

All packages: Both the current user's packages and packages marked public.

User packages: (administrative users only) List of all packages sorted by owner/creator (not including public packages).

Resetting package hashes

The software distribution agent uses the MD5 hash algorithm to verify the package and additional files are downloaded correctly. When a distribution package is first scheduled, the product downloads the files and calculates the hash values associated with the primary file and any additional files used by the distribution package. If the hash stored with the package doesn't match the hash value the agent computed on the target device, the download isn't considered valid. If you make any changes to the package outside of this product, such as updating the package contents, you need to reset the hash, or any scheduled tasks using the updated package will fail.

Cloning

Cloning creates a duplicate of an existing package, such as a package that delivers an executable to a set of targeted devices. If the settings of the package are what you want for another package that will deliver a different executable, you would select the package you want to clone, click **Clone**, and change the executable to be delivered.

About the Scheduled tasks tab

Distribution includes a powerful scheduled task system. Both the core server and managed devices have services/agents that support scheduled tasks. The Management Suite console can add tasks to the scheduler.

A task consists of a distribution package, delivery method, targeted devices, and a scheduled time.

Use the **Scheduled tasks** tab to configure and schedule scripts you've created. Schedule items for single delivery, or schedule a recurring task. For information on the fields, see [Scheduled tasks](#).

Before you can schedule tasks for a device, it must have the standard LANDesk agent and be in the inventory database. LANDesk Server configurations are an exception. They can target a server that doesn't have the standard LANDesk agent.

To schedule a distribution task

1. In the left navigation pane, click **Distribution**.
2. Click **New** to create a package.
3. Click the new package and click **Schedule**.
4. Configure a distribution package and a delivery method.
5. On the **Target devices** page, select the query you created that targets the devices you want. You can also target devices in the target cart by clicking **Add target list**. Targeted devices appear in the lower box.
6. On the **Schedule task** page, configure the schedule.
7. Click **Save**.

When you click **Schedule**, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that it has still been created and appears in the Task list.

About the Delivery methods tab

The **Delivery methods** tab shows you the available delivery methods and any delivery methods that you've configured. When you select a delivery method you've created, you can view the properties for it, delete it, or clone it. The product only supports the Push delivery method. A default push delivery method is created during installation.

Delivery method groups

My delivery methods: Delivery methods that the current user has created. The administrative users can also see these delivery methods.

Public delivery methods: Delivery methods that users have marked common. Anyone who schedules a delivery method from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.

All delivery methods: Both the current user's delivery methods and delivery methods marked public.

User delivery methods: (administrative users only) List of all delivery methods sorted by owner/creator (not including public delivery methods).

For more information on software distribution, see [Software distribution overview](#).

To create a new delivery method

1. In the left navigation pane, click **Distribution**.
2. In the lower pane, click the **Delivery methods** tab, select a delivery method type from the left pane, and click **New**.
3. Type a name for the method in the **Name** text box.
4. In the left pane, select other pages from which to select options. Use **Description** to add descriptive text about the delivery method and change the owner if you want. The **Reboot** page specifies whether to reboot the device after the delivery is complete. The **Discovery** page is used to verify the target computer is configured properly to accept the distribution package.
5. When finished, click **Save**.

About the Description page

Use this page to describe the delivery method you're creating and to set the number of devices you want to distribute to simultaneously.

- **Owner:** Allows users to share methods by setting them to the public owner.
- **Description:** The description you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer names.

About the Reboot page

Use this page to configure whether the computer is rebooted after the software has been installed or removed. You have three options:

- **Never reboot:** Devices won't reboot after a package installation. If you select this setting and your package requires a reboot, devices may encounter errors running the application until they do reboot. If the package is an SWD package, this option overrules any settings in the package. If the package is a generic executable or an MSI package, the package setting may overrule this option.
- **Reboot only if needed:** Devices will reboot if the package requires it.
- **Always reboot:** Devices will reboot regardless of whether the package requires it or not.

About the Discovery page

This page allows you to choose options for device discovery. Before the scheduled task handler can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

Discovery options:

- **UDP:** Selecting UDP uses a Ping Discovery Service (PDS) ping via UDP. Most Server Manager device components depend on PDS, so your managed devices should have PDS on them. PDS is part of the standard LANDesk agent. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping retries and timeout.
- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Number of retries:** The number of attempts discovery makes to contact devices.
- **Discovery timeout:** The number of milliseconds before discovery retries will timeout.
- **Timeout for subnet broadcasts:** The number of milliseconds before subnet broadcast retries will timeout.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast. When selected, this will result in a subnet directed broadcast being sent via UDP using PDS.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

Understanding distribution error codes

When a distribution job finishes, the **Scheduled tasks** page will either display success or an explanation of why it failed. In addition, each targeted client has log files that contain information about the distribution. The status and errors are logged to the following files:

- If the error occurred while attempting to access the package, the error is logged in the AICLIENT.LOG file.
- If the error occurred while processing the package (for example, copying files), the error is logged in the INST32.LOG file.
- The SDCLIENT.LOG file contains general summary information about each installation request received from the core server.

These log files are stored on each client. The following table lists the error codes you may encounter in these files.

Error code	Definition
101	The user cancelled the install.
102	File access was denied.
103	The password used isn't valid.
104	No network found, or incorrect path provided.
105	A download error occurred.
106	A socket could not be created.
107	Unable to open an HTTP session.
108	A CFG download error occurred.
109	A save CFG error occurred.
110	No save CFG folder exists.
111	A file access error occurred.
112	A get CFG error occurred.
113	Unable to create a backup CFG.
114	A spawn error occurred because another package is already being installed.
117	The backup directory can't be created.
180	Networking error. Can't initialize.
188	Timed out while downloading over HTTP.
189	HTTP connection aborted.
191	Host not found.
197	HTTP file not found.
201	The UNC file cannot be found.
202	The file was not found on the installation disk.
203	Unable to create a file in the specified location.
204	Not enough disk space on the destination drive for installation.
205	An invalid drive was specified, or the drive required for this install was not available.

- 206 The file has a long filename and can't be installed by the 16-bit install program. You still have the option to continue to install other files.
- 207 The specified file is not an executable.
- 208 Multiple uninstall registry entries exist with the same source path.
- 209 Unable to locate the uninstall executable.
- 210 Encountered an invalid compressed file, or HTTP error(s).
- 211 A successful AFXSOCKETINIT command must occur before using this API.
- 212 The network subsystem failed.
- 213 No more file descriptors are available.
- 214 The socket can't be created. No buffer space was available.
- 215 The specified address was already in use.
- 216 The connection attempt was rejected.
- 217 The provided host address was invalid.
- 218 The network can't be reached from this host at this time.
- 219 The attempt to connect timed out without establishing a connection.
- 220 The virtual circuit was aborted due to a timeout or other failure.
- 221 The virtual circuit was reset at the remote site.
- 222 A non-stated HTTP error occurred.
- 223 An HTTP error occurred; the file wasn't open for reading.
- 224 An HTTP error occurred; no content-length setting provided.
- 225 An HTTP error occurred; not enough memory available.
- 226 A memory allocation error occurred.
- 227 Unable to read the file.
- 228 Insufficient memory available.
- 229 The .CFG file has an error at line XX.
- 240 The temporary path specified is invalid. It can't be accessed or created. The target computer has a configuration problem.
- 301 This application has never been installed on this computer; it can't be uninstalled.

Troubleshooting distribution failures

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, test the system for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll out occurs should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

Software distribution provides the ability to distribute packages to a large number of devices at once. If there is a problem with the package, or the software being deployed conflicts with already existing software, you have the ability to cause problems at thousands of devices at once. When planning a deployment using software distribution, take care to not overwhelm the help desk.

Before deploying a new package, test it with some test systems. Ideally, these test systems should include all of the operating systems and applications that are used in your environment. Once the package is deployed, confirm that all of the systems and applications are still working as expected.

Once the package has been validated against test systems, do a limited deployment. Target a small number of devices in your environment. When deciding how many devices to target, the rule of thumb is not to target more devices than your help desk can handle. Once the package has been deployed to these devices, let the software sit for a couple of days to see if users encounter any problems.

After the initial deployment, you can begin rolling out the software to other devices in the enterprise. The speed at which these roll outs occur should be based upon how much device variety the enterprise has and how much of a load the help desk can handle.

Here are some other problems you might encounter:

Scheduled task can't find package

If the scheduled task indicates that the package can't be located, make sure that the package can be viewed from the device.

If the package is URL-based, you can check to make sure it is accessible by using a Web browser. Remember, if your DNS is set up to resolve the package, you'll need to verify that the package has been distributed to all of the Web servers.

If the package can be viewed from the device but still does not download properly, the problem may be that the URL or UNC based package share doesn't allow anonymous access. Check the permissions on the UNC or URL share and make sure it allows anonymous access. For UNC locations, make sure it has properly been configured as a null session share.

Bandwidth detection doesn't work

One of the most common problems that can occur is having PDS set up for bandwidth detection. In device setup, one of the common base agent options is to choose between PDS and ICMP for device bandwidth detection. When a device is configured to use PDS for bandwidth detection, it will only detect between RAS and non-RAS connections. So, if you configure a distribution to only work with high speed connection and the package installs on a computer with a WAN connection, check and make sure it is configured to use ICMP and not PDS.

Scripting

Scripting overview

The Package Builder wizard steps you through the process of creating a software distribution package. The wizard saves the commands required to perform the same installation on other computers. It writes these commands to an ASCII file with a .CFG extension. You can edit this script file after creating it in Package Builder, or you can create one from scratch and build it into a package.

The Package Builder online help provides syntax information for each of the script commands. To access the help for a specific command, highlight a command in the left panel and press the **F1** key.

To access a specific script file, start Package Builder and click **File | Open**.

Once a script has been modified, click **Build | Build** to build the script into a package.

Script commands

Each script includes two sections. Specific commands at the top of the script define the operating parameters, and the balance of the commands describes the installation of the application included in the software distribution package.

All of the commands included in a script can be grouped into one of these functional categories:

- Base Installation
- Appearance
- Messages & Input
- System Changes
- If Conditions
- Defaults & Calls

These categories contain related commands that describe the installation process for each package. Some commands describe the operating parameters of the installation and must be placed at the top of the script file. For details about each command, see the Package Builder online help.

Editing packages with the Package Builder

The Package Builder interface is divided into three areas:

- In the left pane, the functional categories are listed. Expand each functional category to display the individual commands within that category.
- The right pane is divided into two screens: The upper portion displays the script itself. The lower portion is a GUI template that contains entry boxes for the parameters of the highlighted command.

To see the details of a command in the script, highlight the command and view the parameter details in the lower portion of the screen.

To add a new command to the script, select the location in the script where the command should be located. Next, highlight the command in the left pane. Now complete the syntax template in the lower portion of the screen. When you've selected the command parameters, click **Add** to insert the new command.

Using scripting commands

Don't pass variables to the DLL Load command in Package Builder

If you create a package that depends on passing a variable into the DLL Load command, it won't work if the variable doesn't arrive at the correct time. If the .DLL doesn't receive the expected variable, the package won't complete the installation correctly. To avoid this problem, don't pass variables into the DLL Load command; the other DLL parameters work correctly.

Using the Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands

The Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands require the full path to the executable to run correctly. Also, the RunAtMiddle command must be positioned in the script after the DEFAULTDIR function to work correctly. RunAtStart and RunAtExit commands can be anywhere in the script and will run correctly.

Rebooting during package creation

When using the Package Builder wizard to create a package, you may be prompted to reboot the package-building computer. In many cases, rebooting before completing the package-building process causes the package to improperly install at the client. The application becomes configured for the package-building computer rather than the targeted client. However, in some cases, the reboot is required because the installation program accesses the installation CD after reboot.

You need to test the resulting package to determine whether you can stop the installation process and create the package before the reboot, or whether you need to reboot the package-building computer during the software installation and then continue to create the package.

Creating and naming software distribution packages

Package names can't be changed once they're created

You can't change a package name once you complete the package creation step. If you attempt to directly change the filename, your users can't access that package correctly.

Package names can't include hyphens or periods

If you use hyphens or periods in a package name, the package-creation process will truncate the name when it encounters them. You can still access the package in a script, and users can install it, but the truncated name might be confusing. Don't use hyphens or periods in a package name. You can use the underscore (_) character instead.

We recommend that you create a new working directory each time you begin creating a package. To create this directory, start the Package Builder wizard, and click **Scan Options**. In the Temporary Work Directory box, either type in the full path to a directory or browse to its location. Package Builder prompts you for permission to create a directory that does not already exist.

Store only software distribution packages in your distribution location

You should only keep packages in the Web server location or UNC folder that you set up for software distribution. If you store other types of executable files in this folder, they may be confused with packages when you're creating distribution package scripts. If you create a distribution script for an executable that's not a package, the distribution will fail. Store only software distribution packages in your distribution location.

For more information about creating and modifying packages, see the topic "Working with the Package Builder" in the Package Builder online help.

File collections can't contain more than 296 files

When you create a file collection package, you can add as many as 296 separate files or folders. If you attempt to add more than 296 items, the file collection stops. Files contained in an included folder count as one item, not as separate files.

Simple sample script

This script contains some of the commands used to install Package Builder on a package-building computer. Major sections or commands are described with remarks (REM).

```
REM This is the Package Builder installation
REM Set screen graphics environment
SCREENCOLOR: (0,0,255), (0,0,255)
ANIMATION: "W:\Software\Install\Intel\duck\DISK01.BMP",
"W:\Software\Install\Intel\duck\DISK02.BMP",
"W:\Software\Install\Intel\duck\DISK03.BMP",
"W:\Software\Install\Intel\duck\DISK04.BMP",
"W:\Software\Install\Intel\duck\DISK05.BMP",
"W:\Software\Install\Intel\duck\DISK06.BMP",
"W:\Software\Install\Intel\duck\DISK07.BMP",
"W:\Software\Install\Intel\duck\DISK08.BMP",
"W:\Software\Install\Intel\duck\DISK09.BMP",
"W:\Software\Install\Intel\duck\DISK10.BMP",
"W:\Software\Install\Intel\duck\DISK11.BMP",
"W:\Software\Install\Intel\duck\DISK12.BMP",
"W:\Software\Install\Intel\duck\DISK13.BMP"
SCREENGRAPHIC: "W:\software\INSTALL\Intel\OAKLAN~1.BMP", topleft
REM TITLE: "LANDesk Management Suite", fontsize=25, color=yellow
REM SUBTITLE: "Package Builder", fontsize=18, italic, color=yellow
REM Configure uninstallation options
UNINSTALL: yes, removegroup, packagename="Package Builder"
UninstallBeginPrompt: "Do you wish to remove the LANDesk Management
Suite Package Builder programs and directories from your system?"
UninstallEndPrompt: "LANDesk Management Suite Package Builder programs
and directories have been successfully removed from your system."
REM Check for sufficient disk space before installation
IF DISKSPACE() < 4000K
BEGINFIRSTSCREEN caption="Not Enough Disk Space", Package Builder
requires 4 MB of disk space. Please arrange your hard disk so that a
sufficient amount of disk space is available.
ENDFIRSTSCREEN
REM This is only shown if there is less than 4 MB of disk space.
```

```

ENDIF
REM Define splash screen text
BEGINFIRSTSCREEN caption="LANDesk Management Suite Package Builder",
This installation program will set up LANDesk Management Package
Builder onto your hard disk. Contact your LANDesk Software Customer
Support representative if there are problems setting it up on your
computer.
ENDFIRSTSCREEN
REM Define default directory from which to work. Notice the variable
$ProgFilesDir$ comes from a Windows system environment variable. The
DEFAULTDIR command must be used before any file commands are used.
DEFAULTDIR: "$ProgFilesDir$\Intel\Package Builder", prompt="Please
enter the drive and directory:", caption="Directory Name", text="The
software will install onto your system in a directory. Please accept
the suggested directory location or type in one of your own. Make
certain to provide both a drive letter and the directory name."
REM Add files common to all versions of Package Builder. Only one has
been included in this sample script.
FILE: "CTL3D.000", overwrite=yes,
From="W:\Software\Install\Intel\CTL3D.DLL"
REM Install registry information
BEGINREGISTRY
KEY: new, "HKEY_CLASSES_ROOT\CFG"
VALUE: reg_sz, replace, "Default", "txtfile"
ENDREGISTRY
REM Setup Windows menu items
WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\Builder.exe",
"Package Builder", replace, allusers
WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\Replicator.exe",
"Package Builder wizard", replace, allusers
WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\ENUBLDRI.hlp",
"Package Builder wizard help", replace, allusers
REM Define and display final screen
BEGINLASTSCREEN caption="LANDesk Management Suite Package Builder",
The installation of the Management Suite Package Builder is now
complete.
ENDLASTSCREEN

```

Sample script with more complex commands

This next script is organized into sections with a brief explanation for each. Any applications launched by a RunAtStart or RunAtMiddle command must be closed for the script to continue processing.

The beginning section of this script enables you to include a window title, package name, animated or still graphics, and audio, as well as color and font selections. A RunAtStart command enables you to execute an external application at the beginning of the installation.

Next, the BeginFirstScreen command enables you to inform the user about the installation by displaying a text message. Finally, the Backup command indicates that any files that are to be replaced will be backed up, and the OverWriteFile command indicates that the user will be prompted before any existing files are overwritten.

```

ANIMATION: "C:\WINDOWS\CIRCLES.BMP", "C:\WINDOWS\CARVED~1.BMP",
"C:\WINDOWS\BUBBLES.BMP", "C:\WINDOWS\BLUERI~1.BMP",
"C:\WINDOWS\BLACKT~1.BMP"
RUNATSTART: "c:\program files\accessories\mspaint.exe"

```

USER'S GUIDE

```
TITLE: "Package Builder Functionality Script for Windows 98", bold
INTROSCREEN: "C:\WINDOWS\SETUP.bmp", waittime=5, full
INTROSOUND: "C:\WINDOWS\MEDIA\START.WAV"
SCREENCOLOR: magenta, yellow
SCREENGRAPHIC: "C:\WINDOWS\PINSTR~1.BMP", topleft
FONTNAME: "Tahoma"
BEGINFIRSTSCREEN title="First Screen", caption="Screen #1"
This is the text that appears on the first screen.
ENDFIRSTSCREEN
BACKUP: YES
OVERWRITEFILE: ask
```

The following examples show different prompt options. Text for each prompt can be modified.

```
CancelPrompt: "Cancel?"
CopyFilePrompt: "UPLOAD IN PROGRESS"
OkPrompt: "GOOD JOB"
QuitPrompt: "Do you really want to quit?"
CopyTitlePrompt: "Copying..."
NextPrompt: "Next"
BackPrompt: "Back"
NoPrompt: "No"
YesPrompt: "Yes"
```

This section runs an external application and waits for that application to be closed before continuing. When the script continues, the user is prompted for input. Based on the selected option, the application continues and copies a file on the local drive or exits.

```
RUNATMIDDLE: "c:\windows\calc.exe"
ASK1: Yesno, caption="Sample question.", text="This is an example using
Yes / No buttons. Choose `Yes' to continue, `No' to exit."
IF $ASK1$= "yes"
WINGROUP: "New Program Group", prompt="Select a group",
caption="Program Group selection", text="Please select a program
group."
ELSE
IF $ASK1$= "No"
EXITMESSAGE
Sorry you had to leave so soon!
EXIT
ELSE
ENDIF
ENDIF
PROGRESSBAR: 302K
COPY: "C:\windows\setup.bmp", "C:\windows\temp\p1.bmp"
RENAME: "C:\windows\temp\p1.bmp", "C:\windows\temp\renamed p1.bmp"
```

This section launches an application as the last command before the script is completed. The RunAtExit command does not have to be the last line of the script.

This section also places a shortcut on the desktop and creates an uninstall package.

```
RUNATEXIT: "C:\WINDOWS\CDPLAYER.EXE"
BEGINLASTSCREEN title="Last screen", caption="The last screen"
This should be the last screen you see.
ENDLASTSCREEN
SHORTCUT: "c:\windows\notepad.exe", "NOTEPAD",
dir="c:\windows\desktop\"
UNINSTALL: yes, makeicon, removegroup, packagename="Package Builder
Functionality"
```

Package Builder

Running the Package Builder wizard

As described earlier, building a software distribution package is a two-phase process. The first phase creates an installation script (.CFG file) in the Package Builder working directory. This script contains all the client instructions for installing the software. The second phase builds the software distribution package. The package contains the instructions plus the files.

To run the Package Builder wizard

1. From your package-building computer, click **Start | Programs | LANDesk Management | Package Builder wizard**.
2. Click **Scan options** to configure the scan process. On this page, you can select which directories the wizard monitors for changes and whether the wizard creates a backup to return the client to its present state after the package has been created. When you're finished modifying the form, click **OK**.

At least one logical or physical disk drive must be monitored

The Package Builder wizard needs to monitor at least one logical or physical disk drive to track system information changes. If you clear the default drive selection in the **Scan options** page, and set it to monitor no drives, the wizard will exit.

3. Click **Build options** to configure user-specific settings for Windows NT and Windows 2000/2003/XP systems. You can select to have these settings applied to the logged-in user (or the default user if no one is currently logged in) or to all users. These user-specific settings include Start Menu items, shortcuts, and registry settings for the HKEY_CURRENT_USER key. To return, click **OK**.
4. Click **Next**. The wizard will check out your system.
5. Select the method you want to use to install the application:
 - If the installation program is locally available (such as a SETUP.EXE program), click **Browse** to locate the installation program, select it, and then click **Monitor**.
 - If the installation program is on an autorun CD, click **Next** and insert the CD.
 - To make other types of changes for a software distribution package (such as copying files or creating desktop shortcuts), click **Next** and run the appropriate utility.
6. Follow the prompts to install the software.
7. When the installation is complete, enter a name for the package. We suggest you enter a name that includes both the software and the operating system; for example, WinZip_Win2K for a package that installs WinZip on a Windows 2000/2003 client.
8. Click **Compare**.
9. When the .CFG file has been created, click **OK** and then **Build**.
Note: The .CFG file can be customized and then built into a package.
10. When the build completes, the wizard will put the package in the Onefile folder of the Package Builder Working directory. The package will be an .EXE file with the name you selected. Click **Finish**. You can manually test this package by clicking the .EXE file.

The next task is to set up the delivery server and copy this package to it.

Setting up a package-building computer

The package-building computer should be a dedicated computer with a clean installation of its operating system. The clean installation is necessary because the package-building process captures all elements added or modified on the package-building computer.

Because you can distribute packages only to clients running the same operating system as the package-building computer, you should have a separate package-building computer, or a separate drive partition, for every operating system you distribute to. You can also use a single computer with multiple OS images as your package-building computer.

Any preinstalled software on the package-building computer reduces the Package Builder's ability to recognize changes. For this reason, your package-building computer must be as generic and clean as possible. This rule also applies to the CONFIG.SYS and AUTOEXEC.BAT files and other configuration files that the application installation process may modify.

To install the package-building software

1. From your package-building computer, browse to ENUSETUP.EXE in the LDMAIN\install\Package_Builder folder of the core server.
2. Double-click **ENUSETUP.EXE**, then click **Next**.
3. Type in the location of the folder where you want to install the package-building software, then click **Finish**.

Setup puts three items on the package-building computer:

- **Package Builder wizard:** Used to automatically create software distribution packages. It takes a "before" snapshot of the computer's state, has you install the software, takes an "after" snapshot of the computer's state, and builds a package from the differences in the snapshots.
- **Enhanced Package Builder:** Used to manually create, modify, and edit software distribution packages.
- **Package Builder wizard help:** Online help that describes the Package Builder wizard.

Once the Package Builder software is installed on your computer, you can use this computer to create and edit software distribution packages. The Package Builder stores packages on the local hard disk by default. Once these packages are built, you must move them from the package-building computer to the package share on your delivery server.

Building a package

You can use the Package Builder wizard to automate the process of taking snapshots and compiling them into standalone packages. As shown below, the process includes four steps:

1. Taking a pre-installation snapshot
2. Installing the application or making a computer configuration change
3. Taking a post-installation snapshot
4. Restoring the package-building computer

1. Taking a pre-installation snapshot

To build a software package, use the Package Builder to scan the local hard drive. You can specify exactly which portions of the drive are scanned in the Scanning Options page. This scan checks the system registry and all the directories and files on the local computer. After you install new software on the system, the Package Builder uses this information to detect what changes were made to the computer; it then compiles these changes to create the software distribution package. This information is stored in the temporary work directory. Specify this directory in the Scan Options page of the Package Builder wizard.

Package Builder scans all local drives by default. If you don't plan to make any changes to a local drive during the installation, remove it from the scan to speed up the pre-scan process. For best results, allow the Package Builder to scan the drive partition where the operating system is stored, plus the drive where you intend to install the software or change the configuration.

If, at any time during the package-building process, the hard drive space on the package-building computer gets low, the Package Builder will stop, display a warning, allow you to provide more drive space, then continue the package-building process.

Even if you remove all the local drives from the scan list, the Package Builder still scans the system files and folders, as well as the computer's registry.

2. Installing the application or making a computer configuration change

Once the pre-installation snapshot is created, the Package Builder prompts you to install the application software to distribute as a package.

You can install multiple applications in a single package, but you should install only suite-type applications with this process. If you install multiple applications as one distribution package and later want to omit one, you must first remove the entire group and then install a new group of applications. If you want to install multiple packages to your managed clients, you should edit the software distribution script so that it installs several different packages during the distribution.

The Package Builder monitors the installation during this step, then waits until the installation is finished to continue with the wizard pages. You can then customize the finished program. For example, if the install program creates an uninstall icon that you prefer not to distribute to clients, you can delete the icon before the post-installation snapshot in step 3, omitting it from the package. You can also add new icons to specific program groups, which provides a single point of access for all your users.

You need to provide any setup information requested by the system, and answer all questions presented during the software setup. The Package Builder cannot perform these tasks for you, but it will save the information as part of the package.

If you want to change only some of the system settings on clients, or if you want to copy a collection of specific files, you can create a package without using the snapshot process.

When you're satisfied that the application software or the configuration changes are ready, return to the wizard and click Next to start the post-installation snapshot.

3. Taking a post-installation snapshot

In this step, the Package Builder takes a second snapshot of the package-building computer and compares it with the pre-installation snapshot. By analyzing the differences, the Package Builder can identify any changes that have occurred on the computer, and then build a package distribution configuration script. This file has a .CFG file extension, and is located in the c:\Program Files\LANDesk\Package Builder\ folder on the package-building computer.

This .CFG script file describes the changes to the registry, the file system, the desktop, and other system resources. It does not create a removal control file however, so you must add an uninstall option manually, either when you edit the script or when you schedule it for distribution.

Once these changes are saved, the Package Builder wizard offers the option to compile the .CFG file into an executable file, or to open it in Package Builder to make additional changes. Click Edit to open the new .CFG file in Package Builder and make your modifications. When you're satisfied with the installation, click Build to create the package.

Once finished, a page appears showing that the package was created and stored in the default directory on the package-building computer.

4. Restoring the package-building computer

Once you finish the package-building session, you should restore the package-building computer to its pre-installation state. This process ensures that the computer is in a clean state for the next package build. SWD doesn't include a process for restoring the computer to a clean state; therefore, you should use a computer-imaging program such as the LANDesk imaging tool that is part of OS Deployment, Symantec's Ghost*, and so on to restore the client's operating system.

If you use a utility like Ghost to restore the package-building computer, you will also delete the .CFG file that was used to create the package. If you want to keep these files available, either to use in future packages or to edit at a later time, you can store them on a network share drive. Just specify a network location in the Scan Options page of the wizard to preserve these files.

By default, each new system scan is stored in a new working directory, but you can use the same folder again if you prefer to overwrite the old system scan. Some users keep software images of multiple operating systems on a single package-building computer. This solution provides optimum flexibility when creating software packages, without dedicating multiple computers specifically for software package building.

Launching a package from a package

You can specify INST32.EXE on the command line of a RunAtExit command in one package in order to launch another package. The syntax is:

```
RunAtExit "INST32.EXE PACKAGENAME.EXE"
```

If the package is found on the network, this is more efficient than just running "PACKAGENAME.EXE." It allows you to specify a package name via an HTTP path. For example:

```
http://myservername/packages/PACKAGENAME.EXE
```

Using the Package Builder online help

For detailed instructions about creating and modifying .CFG files, see the Package Builder online help. Click **Start** | **Programs** | **LANDesk Management** | **LANDesk Enhanced Package Builder**. Click **Help** | **Index** and select the following online help topics:

- Getting started with Package Builder
- Creating a simple installation
- Package Builder commands
- How does Package Builder do an installation?
- Using variables in commands and assigning values

Modifying the registry

Commands that modify the registry begin and end with BeginRegistry and EndRegistry commands. In between these commands are the commands that identify the registry key and the value. The Package Builder wizard flags two keys as dangerous:

- \HARDWARE
- \SYSTEM\CURRENTCONTROLSET

These keys are considered dangerous because they are usually not compatible with any computer other than the package-building computer. When these keys are modified, the Package Builder wizard places such commands within an IF \$DANGEROUS\$ = "TRUE" statement. If the changes to these keys are compatible with your target computers and you want them executed, you must define a \$DANGEROUS\$ variable at the top of the script and set its value to TRUE.

Scripts

Managing scripts

This product uses scripts to execute custom tasks on devices. Completing the script creation dialogs generates an ASCII text file in the Windows INI format with an .INI extension. These scripts are stored on the core server in the \Program Files\LANDesk\ManagementSuite\Scripts folder. The script filename becomes the script name in the console.

The Scripts window divides scripts into the following categories:

- **My scripts:** Scripts that you created.
- **All OSD scripts:** All OS deployment scripts, created from the OS deployment feature.
- **All other scripts:** Scripts that shipped with the product.
- **User scripts** (only visible to administrators): Scripts created by all product users. These are sorted by creator.

You can create groups under the **My scripts** item to further categorize your scripts.

File transfer and local scheduler scripts are not supported in Linux. Vulnerability scanner scripts (except remediation scripts) and software distribution scripts (for the distribution of RPMs) are supported.

Once you've created a script, you can click **Schedule** on the script's shortcut menu. From the **My devices** window, you can target devices the task should run on, and you can schedule when the task should run from the **Scheduled tasks** window. See the next section for more information on scheduling tasks.

Due to specific capabilities supported by the Windows console, scripts created in the Windows console should not be edited in the Web console.

Changes to script and task ownership for users of previous Management Suite versions

With Management Suite versions prior to 8.6, all scripts were global and all users could see them. Now scripts are only visible to the script creator and to administrators.

The **Scripts** window has a State column. The State column shows Public if all users can see the script, or Private if only the user that created the script or administrators can see it. Users can right-click scripts they have created and click Private or Public to change a script's state. Administrators can change the state of any script.

Scheduling scripting tasks

The **Scheduled tasks** window shows scheduled task status and whether tasks completed successfully or not. The scheduler service has two ways of communicating with devices:

- Through the standard LANDesk agent (must already be installed on devices).

- Through a domain-level system account. The account you choose must have the log in as a service privilege and you must have specified credentials in Configure services. For more information on configuring the scheduler account, see Configuring the scheduler service.

LANDesk installs several standard scripts that you can schedule to perform routine maintenance tasks such as running inventory scans on selected devices. Click **Scripts** in the left navigation pane, then click **All other scripts** to view and schedule these scripts.

To schedule a task

1. In the left navigation pane, click **Scripts**.
2. Click to navigate to the script group.
3. Click a script, and click **Schedule**.
4. Type a name for the task, and click **OK**.
5. In the **Custom script tasks** tab, click **All tasks**, click the task you named in step 3, and click **Edit**.
6. Fill out the pages of the custom script task. Click the Help button for help on any page, or see the Task scheduler help.

When you click **Schedule**, a task is created (it has no targeted devices, and it is unscheduled). If you cancel this Scheduled task procedure, please be aware that it has still been created and appears in the Task list.

Using the default scripts

This product ships with several default scripts. You can use them to help you complete some typical tasks. These scripts are available under the All other scripts tree in the **Scripts** window (left navigation pane | **Scripts**) with the exception of the Generic sample dir command script, which is available under **All OSD scripts**. If you did a dual install with LANDesk Management Suite, there may be additional predefined scripts.

- **Generic sample dir command:** Uses an OS deployment script to demonstrate running a dir command.
- **inventoryscanner:** Runs the inventory scanner on the selected devices.
- **MSI service deployment:** Deploys the MSI service required for a PXE representative.
- **PXE representative deployment:** Deploys or updates a PXE representative.
- **PXE representative removal:** Removes the PXE service software from a PXE representative.
- **Restore client records:** Runs the inventory scanner on selected devices, but the scanner reports to the core the device was configured from. If you have to reset the database, this task helps you add devices back to the proper core database in a multi-core environment.

Scheduling tasks

- Target devices page
- Schedule task page
- Credentials page
- Image Information page
- Additional commands page
- LANDesk agent page
- DOS commands page
- Custom scripts page

The Scheduled tasks tool is common to Configure agents, Scan vulnerabilities, Distribute software, Discovery, Scripts, and OS deployment. The tasks are filtered in the lower pane of the specific feature pages to show only related tasks. For example, if you open the Discover devices tool, discovery tasks are displayed in the Discovery tasks tab in the lower pane of the Discover devices page. All tasks are still visible through the Scheduled tasks tool. Here you can schedule configurations to run immediately, at some point in the future, on a recurring schedule, or run just once.

The left pane of the Scheduled tasks page shows these task groups:

- **My tasks:** Tasks that you have scheduled. Only you and administrative users can see these tasks.
- **All tasks:** Both your tasks and tasks marked public.
- **Common tasks:** Tasks that users have marked common. Anyone who schedules a task from this group will become the owner of that task. The task remains in the Common tasks group and will also be visible in the User tasks group for that user.
- **User tasks** (administrative users only): Tasks users have created.

When you click My tasks, Common tasks, or All tasks, the right pane shows this information:

- **Task:** The task names.
- **Start On:** When the task is scheduled to run. Click a task name and click **Edit** to edit the start time or to reschedule it.
- **Status:** The overall task status. View the right pane Status column for more details. The right pane column shows the task status, which can be Working, All Completed, None Completed, or Failed.
- **Distribution package:** The package name the task distributes.
- **Delivery method:** The delivery method the task uses.
- **Owner:** The name of the person who originally created the script this task is using.

When you double-click a scheduled task, the right pane shows this summary information:

- **Name:** The task state name.
- **Quantity:** The number of devices in each task state.
- **Percentage:** The percentage of devices in each task state.

Before you can schedule tasks for a device, it must have the appropriate agent and be in the inventory database. Server configurations are an exception. They can target a device that doesn't have the standard LANDesk agent. Tasks can be rescheduled (edited) or deleted from the Tasks tabs. Once you schedule a task, see the Tasks tab for task status.

You can edit a task by selecting the task you want to edit and clicking **Edit**. The task opens with editing options applicable to the task.

About the Target devices page

Use this page to add device targets for the task you're configuring. You can also see the targeted devices, queries, and device groups for the task on this tab. Device groups are created in Management Suite, and are viewable in Management Suite. This page is not needed for Discovery tasks.

- **Add target list:** Add the devices previously put in the target list from My devices.
- **Add query:** Targets the results of a query that you've previously created.
- **Remove:** Removes the selected targets.

About the Schedule task page

The Scheduler contains a Scheduled task – properties tab that includes these options.

- **Leave unscheduled:** (default) Leaves the task in the Task list for future scheduling.
- **Start now:** Runs the task as soon as possible. It may take up to a minute for the task to start.
- **Start later:** Starts the task at the time you specify. If you click this option, you must enter the following:
 - **Time:** The time you want the task to start
 - **Date:** The date you want the task to start. Depending on your locale, the date order will be day-month-year or month-day-year.
 - **Repeat every:** If you want the task to repeat, click whether you want it to repeat **Daily**, **Weekly**, or **Monthly**. If you pick **Monthly** and the date doesn't exist in all months (for example, 31), the task will only run in months that have that date.
- **Schedule these devices:** For the first time a task runs, you should leave the default of Waiting or currently working. For subsequent runs, choose from All, Devices that didn't succeed, or Devices that didn't try to run the task. These options are explained in more detail below.
 - **All:** Select this if you want the task to run on all devices, regardless of state. Consider using this option if you have a task, especially a repeating one, that needs to run on as many devices as possible.
 - **Devices that didn't succeed:** Select this if you only want the task to run on all devices that didn't complete the task the first time. This excludes devices that have a Successful state. The task will run on devices in all other states, including Waiting or Active. Consider using this option if you need the task to run on as many unsuccessful devices as possible, but you only need the task to complete successfully once per device.
 - **Devices that didn't try to run the task:** Select this if you only want the task to run on devices that didn't complete the task and didn't fail the task. This excludes devices that were in an Off, Busy, Failed, or Canceled state. Consider using this option if there were a lot of target devices that failed the task that aren't important as targets.

About the Credentials page

- **Username:** Identifies a user account with credentials required for the user to log on to the network share.

- **Password:** Provides the user's password.
- **Domain:** Provides the user's Active Directory domain.

About the Image information page

Use this page to specify the type of image you want to restore with this script, where the image is stored, and where the imaging tool is located:

- **Image type:** Identifies the file type (format) of the existing image file you want to deploy with this script, selected from the list of imaging tools.
- **UNC path to image file to restore:** Locates the server and share where the image file is stored, including the image filename. The image must be stored on a share accessible to devices.
- **UNC path to imaging tool:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename.

About the Additional commands page

- **Enter commands to run before the device is rebooted and imaged:** Enter commands to be executed prior to the device being rebooted and imaged.
- **Enter additional command line parameters for the imaging tool:** Enter any additional parameters not previously specified.

About the LANDesk Agent page

- **UNC path:** The path to the agent package.
- **Username:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password:** Provides the user's password.
- **Domain:** Provides the user's Active Directory domain.

About the DOS commands page

- **DOS commands:** Enter DOS commands you want to be executed on the device at the time of the deployment.
- **Abort this job if any command fails:** Stops the task should any command fail to execute and restores the device to its previous state.

About the Custom scripts page

- **Currently selected custom script:** Select the script you want to schedule.

Reports

About reports

Management Suite includes a reporting tool you can use to generate a wide variety of specialized reports that provide critical information about the managed devices on your network.

Management Suite uses an inventory scanning utility to add devices (and collected hardware and software data about those devices) to the core database. You can view and print this inventory data from a device's inventory view, as well as use it to define queries and group devices together. The reporting tool takes further advantage of this scanned inventory data by collecting and organizing that data in useful report formats.

You can use the predefined Management Suite service reports and inventory asset reports. After running a report, you can view it from the Server Manager console.

If you have Management Suite and Management Suite installed together, the reports you run in Management Suite will only include servers. If you run a query you will get both servers and other devices, unless the query has been configured to exclude other devices.

Understanding report groups and predefined reports

Reports are organized in groups in the **Reports** window (left navigation pane | **Reports**). Administrators can view the contents of all of the report groups. Server Manager includes a specific role, called Reporting, to allow others to view Management Suite reports without providing them access to other management capabilities. (For more information, see Role-based administration.) Users with the Reporting right can also see and run reports, but only on the devices included in their scope.

The **Reports** window has the following groups of reports:

- Hardware
- Software
- Other

Viewing reports

You can run any report from the **Reports** window.

From the **Reports** window, click a report group, then click the report you want to run. The report data displays in the **Report view**.

About the Report view window

Reports allow you to quickly access a graphical representation of the assets on your client computers. The reports are created from data the scanner stores in the database. You can view reports or print them through your browser.

To view a report

1. In the left navigation pane, click **Reports**. Report categories are listed in the right pane. Click a category heading to view the list of reports. An icon next to each report indicates the report type.



A report with a chart icon next to it displays as a pie or bar chart (two- or three-dimensional). In a chart, you can click on any colored bar or pie section to drill down to a summary.



A report with a document icon next to it displays as text.

2. Click the report name to view the report.
3. For the hardware or software scan date summaries, click the start and end dates to set the time frame, then click **Run**.

The Disk Space Summary report contains data for Windows-based servers only.

To print a report, right-click the page and click **Print**. On the Print dialog, click **Print**. If a report spans multiple pages, you must right-click in each page to print it.

To distribute a report

- To e-mail a report, the recommended method is to print the report to a .PDF file, then attach it to the e-mail.

The console displays report charts as pie or bar charts. To set the chart type, click the drop-down list in the report chart, then change the chart type.

In order to view the interactive bar and pie charts displayed in many reports, you must have Macromedia Flash Player* 7 installed.

Queries

Using queries

Queries are customized searches of your core databases. Management Suite provides tools that let you create *database queries* for devices in your core database, as well as a method for you to create *LDAP queries* for devices located in other directories. You create core database queries in the console's **Query** view. Management Suite public queries are visible in LANDesk Management Suite, and vice-versa, if both are being used. You create LDAP queries with the **Directory manager** tool.

Read this section to learn about:

- Queries overview
- Query groups
- Creating database queries
- Running queries
- Importing and exporting queries

Queries overview

Queries help you manage your network by allowing you to search for and organize devices in the core database based on specific system or user criteria.

For example, you can create and run a query that captures only devices with a processor clock speed of less than 166 MHz, or with less than 64 MB of RAM, or with a hard drive of less than 2 GB. Create one or more query statements that represent those conditions and relate statements to each other using standard logical operators. When the queries are run, you can print the results of the query, and access and manage the matching devices.

If you have Management Suite and Management Suite installed together, the reports you run in Management Suite will only include servers. If you run a query you will get both servers and other devices, unless the query has been configured to exclude devices.

Query groups

Queries can be associated with groups in the **My devices** view. These are called dynamic groups, and the contents of a dynamic group are the result of the query associated with that dynamic group. For example, a group comprising all the devices in a geographic area can be associated with a query on memory, hard disk size, and so forth.

For more information on how query groups and queries display in the **All devices** view, and what you can do with them, see Grouping devices for actions.

Creating database queries

Use the **New query** dialog to build a query by selecting from attributes, relational operators, and attribute values. Build a query statement by choosing an inventory attribute and relating it to an acceptable value. Logically relate the query statements to each other to ensure they're evaluated as a group before relating them to other statements or groups.

To create a database query

1. In the console's **Queries** view, click **New**.
2. Select a component from the inventory attributes list.
3. Under **Step 1: Search conditions**, click **Edit**.
 1. Drill down this list to select the attributes that will be your search condition. For example, to locate all clients running a particular type of software, you would select `Computer.Software.Package.Name`.
 2. After selecting the attributes, you'll notice that a series of fields appear in the right side of the window. From these fields, select an operator and value to complete the search condition. For example, to locate all clients running Internet Explorer 5.0, the attributes would be `"Computer.Software.Package.Name,"` the operator `"=,"` and the value `"Internet Explorer 5."`
 3. At the bottom of the window, click **Add** to fill in the empty field with your search condition.
 4. You can continue to refine the query by creating another search condition, then adding it to the first with a boolean operator (AND or OR). Also use the buttons to add, delete, replace, group, or ungroup the conditions you create.
 5. When you're finished, click **OK**.
4. Under **Step 2: Attributes to display**, click **Edit**.
 1. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query. If you cannot find attributes you want to display, you can add them in the Custom attributes dialog. However, these attributes must be assigned to machines before they appear in the query dialog.
Note: If you're using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, `Computer.Display Name`, `Computer.Device Name`, `Computer.Device ID`, `Computer.Login Name`, and so on).
 2. After you've selected an attribute, click **>>** to move it into the empty field on the right side of the window. If you want to enumerate your query results list, click **Include count**.
 3. Repeat the process if you want to add more attributes. Use the arrow buttons to add or remove attributes, and click **Move up/Move down** to change the order of attributes.
 4. Click **Make results targetable** to enable the results of the query to be targetable for any actions you specify.
 5. When you're finished, click **OK**.
5. (optional) Under **Step 3: Sort results by attribute**, click **Edit** to customize the order of query results.
6. If you want to run the query additional times, click **Save query**, and enter a unique name for the query. If you run the query prior to saving it, the query parameters are lost and must be reconstructed to run the same query again.
7. Under **Step 4: Run query**, click **Run query**.

About the New query dialog

Use this dialog to create a new query with the following functions:

- **Name:** Identifies the query in query groups.
- **Machine components:** Lists inventory components and attributes the query can scan for.
- **Relational operators:** Lists relational operators. These operators determine which description values for a certain component will satisfy the query.

The Like operator is a new relational operator. If a user doesn't specify any wild cards (*) in their query, the Like operator adds wildcards to both ends of the string. Here are three examples of using the Like operator:

Computer.Display Name LIKE "My Machine" queries for: Computer.Display Name LIKE "%Al's Machine%"

Computer.Display Name LIKE "Al's Machine*" queries for: Computer.Display Name LIKE "Al's Machine%"

Computer.Display Name LIKE "**Al's Machine" queries for: Computer.Display Name LIKE "%Al's Machine"

- **Display scanned values:** Lists acceptable values for the chosen inventory attribute. You can also manually enter an appropriate value, or edit a selected value, with the **Edit values** field. If the selected relational operator is Exists or Does Not Exist, no description values are possible.
- **Logical operator:** Determines how query statements logically relate to each other:
 - **AND:** Both the previous query statement AND the statement to be inserted must be true to satisfy the query.
 - **OR:** Either the previous query statement OR the statement to be inserted must be true to satisfy the query.
- **Insert:** Inserts the new statement into the query list and logically relates it to the other statements according to the listed logical operator. You can't choose this button until you've built an acceptable query statement.
- **Edit:** Lets you edit the query statement. When you're finished making changes, click the **Update** button.
- **Delete:** Deletes the selected statement from the query list.
- **Clear all:** Deletes all statements from the query list.
- **Query list:** Lists each statement inserted into the query and its logical relationship to the other listed statements. Grouped statements are surrounded by parentheses.
- **Group ():** Groups the selected statements together so they're evaluated against each other before being evaluated against other statements.
- **Ungroup:** Ungroups the selected grouped statements.
- **Filters:** Opens the **Query filter** dialog that displays device groups. By selecting device groups, you limit the query to only those clients contained in the selected groups. If you don't select any groups, the query ignores group membership.
- **Select columns:** Lets you add and remove columns that appear in the query results list for this query. Select a component, and then click the right-arrow button to add it to the column list. You can manually edit the Alias and Sort Order text, and your changes will appear in the query results list.
- **Save:** Saves the current query. When you save a query before running it, the query is stored in the core database and remains there until you delete it.

Query statements are executed in the order shown

If no groupings are made, the query statements listed in this dialog are executed in order from the bottom up. Be sure to group related query items so they're evaluated as a group; otherwise, the results of your query may be different than you expect.

Running queries

To run a query

1. In the **All devices** view, expand the query groups to locate the query you want to run.
 2. Right-click the query and select **Run query**.
- Or
3. To make changes to the query before running it, double-click the query, modify steps 1-3, and then click **Run query**.

Note: If you have modified the query and want to save your changes, click **Save query** to save the changes or **Save query as** to give the modified query a new name. Do this before running the query. If you do not save your changes before running the query, the changes will not be saved with the query.

4. The results (matching devices) display in the right-hand pane of the **All devices** view.

Importing and exporting queries

You can use import and export to transfer queries from one core database to another. You can import Management Suite exported queries as .XML files.

To import a query

1. Right-click the query group where you want to place the imported query.
2. Select **Import** from the shortcut menu.
3. Navigate to the query you want to import and select it.
4. Click **Open** to add the query to the selected query group in the **All devices** view.

To export a query

1. Right-click the query you want to export.
2. Select **Export** from the shortcut menu.
3. Navigate to the location where you want to save the query (as an .XML file).
4. Type a name for the query.
5. Click **Save** to export the query.

Understanding custom queries

Custom queries are useful when you want inventory details about hardware and software installed on your devices. Use a custom query to build a list of computers that have similar inventory. Custom queries are also used to define groups and scopes.

The **Custom queries** page (click **Queries** in the left navigation pane) displays a list of queries that you have saved. To run a saved query, select the query, then select **Run**.

If the query list spans multiple pages, use the arrows at the top of the page to navigate between pages. Enter the number of items to display per page and click **Set**.

Creating custom queries

Custom queries are useful when you want inventory details about hardware and software installed on your devices. Use a custom query to build a list of devices with similar inventory. For example, if you want to upgrade all devices to at least a 750 MHz processor, you can query for all devices in your database with processor speeds of less than 750 MHz. Custom queries are also used to define groups and scopes.

You can query on any of the inventory items (known as "attributes") that the inventory scanner stores in the database, as well as any custom attributes.

Managing queries

Manage queries in the **Queries** view. Use this view to create, edit, or delete queries:

- To run an existing query, select it and click **Run**.
- To create a new query, click **New**. Once you have created and saved that query, its name will appear in the list on this page.
- To edit a query in the list, double-click it. The **Edit query** page appears with query parameters you can edit.
- To edit the most recent query, click **Edit current query**.
- To delete a query, select the query and click **Delete**.

Creating a query is a four-step process:

1. **Create a search condition:** Specify a set of inventory attributes that will be the basis of your query.
2. **Select attributes to display:** Refine or "filter" the query so that the results display the attributes most useful to you, such as IP addresses or computer device names.
3. **Sort results by attributes (optional):** Specify how you want the query results sorted. (Only applies if, in Step 2, you selected to display more than one type of attribute in the query results.)
4. **Run the query:** Run the query you just created. You can also save it for later use, or clear all of the query information to begin again.

Step 1: Creating a search condition (required)

A search condition is a set of inventory attributes and associated values that you query for. You can use one search condition or group several together to form the basis of a query.

The following steps take place on the **Edit query** page. From the **Run queries** view, click **New**, or select an existing query and click **Edit**.

To create a search condition

1. Under **Step 1**, click **Edit**. A window appears showing a list that represents all of the inventory data currently in the database.
2. Drill down this list to select the attributes that will be your search condition. For example, to locate all clients running a particular type of software, you would select `Computer.Software.Package.Name`.
3. After selecting the attributes, you'll notice that a series of fields appear in the right side of the window. From these fields, select an operator and value to complete the search condition. For example, to locate all clients running Internet Explorer 5.0, the attributes would be "`Computer.Software.Package.Name`," the operator "=", and the value "Internet Explorer 5."
4. At the bottom of the window, click **Add** to fill in the empty field with your search condition.
5. You can continue to refine the query by creating another search condition, then adding it to the first with a boolean operator (AND or OR). Also use the buttons to add, delete, replace, group, or ungroup the conditions you create.
6. When you're finished, click **OK**.

To run and store a query on the health status of servers (`Computer.Health.State`), you should be aware that the state in the database is represented by a number. Use the table below to create search conditions. For example, to create a search condition for machines with "Unknown" health, use the operator "NOT EXIST."

Health condition	Operator
Unknown	NOT EXIST
Normal	2
Warning	3
Critical	4

Step 2: Selecting attributes to display (required)

For Step 2, select the attributes that will be most useful for identifying computers returned in the query results. For example, if you want results that help you physically locate each computer matching the search condition set in Step 1, you would specify attributes such as each computer's display name (Computer.DisplayName) or IP address (Computer.Network.TCPIP.Address).

The following steps take place on the **Edit query** page.

To select attributes to display

1. Under **Step 2**, click **Edit**. A window appears showing a list that represents all of the inventory data currently in the database.
2. Drill down this list to select an attribute to display in the query results list. Remember to select attributes that will help you identify the clients returned in the query. If you cannot find attributes you want to display, you can add them in the Custom attributes dialog. However, these attributes must be assigned to machines before they appear in the query dialog.
Note: If you're using an Oracle database, make sure you select at least one attribute that is natively defined by the inventory scanner (for example, Computer.Display Name, Computer.Device Name, Computer.Device ID, Computer.Login Name, and so on).
3. After you've selected an attribute, click **>>** to move it into the empty field on the right side of the window. If you want to enumerate your query results list, click **Include count**.
4. Repeat the process if you want to add more attributes. Use the arrow buttons to add or remove attributes, and click **Move up/Move down** to change the order of attributes.
5. Click **Make results targetable** to enable the results of the query to be targetable for any actions you specify.
6. When you're finished, click **OK**.

You can also add column heading(s) to your query results list.

To change column headings (optional)

1. Under **Step 2**, click **Edit**.
2. In the bottom box, click a column heading and click **Edit**. Edit the heading and press **Enter**. Repeat as necessary.
3. Click **OK**.

At this point, you may want to save your query; the next procedure in the query-creation process is optional and applies only to query results that contain two or more columns. To save your query, click **Save Query** at the top of the page. A window appears prompting you to type a name for this query. Type a name, then click **Save** in the top right corner of the window.

Step 3: Sorting results by attribute (optional)

This procedure is necessary only if you defined more than one attribute and column heading in Step 2 and now want to sort the results alphabetically or numerically within one of those columns.

For example, let's say you specified two different attributes to display in the query results: the IP address and the processor type of each returned computer. In Step 3, you could sort alphabetically by processor type in the results.

If you skip this step, the query will automatically sort by the first attribute selected in Step 2.

To sort results by attribute

1. Under **Step 3**, click **Edit**. A window appears showing the attributes you selected in **Step 2**.
2. Select which attribute you want to sort by, then click **>>** to move it over to the empty text box.
3. Click **OK**.

Step 4: Running the query

After creating your query, you can run, save, or clear it to start over.

To save the query for future use, click the **Save** toolbar button. The query now appears in the list on the **Custom queries** page. If your query is a modified version of another, click the **Save as** toolbar button to give it a new name.

By default, saved queries are only visible by the person who saved them. If you check **Public query** before saving, the saved query will be visible to all users. Only administrators with the public query management right can make a query public.

Management Suite and Management Suite share queries. If you save a query in Management Suite, it will also be visible in Management Suite, and the reverse is true too.

To view the results of this query, click the **Run** toolbar button.

To clear the query parameters from the **Edit query** page, click the **Clear** toolbar button. If the query has already been saved, it's cleared from this page but remains in the **Custom queries** list.

Viewing query results

Query results match the search criteria you specified in the query-building process. If the results aren't what you expected, go back to the **Edit query** page and refine the information.

To drill down to more information about one of the devices in the list of query results, double-click the query data or right-click and click **View computer** in the resulting menu.

From the **Query results** page, you can click the **Save as CSV** toolbar button to export the results into a format compatible with spreadsheet or other applications.

To print the query results, click **Print view** in the query results page.

Viewing drill-down query results

Query results match the search criteria you specified in the query-building process. If the results aren't what you expected, go back to the **Edit query** page and refine the information.

To drill down to more information about one of the devices in the list of query results, double-click the query data or right-click and click **View computer** in the resulting menu.

Exporting query results to CSV files

To view your query results data in a spreadsheet application, export the data as a comma-separated values (CSV) file. From the **Query results** page, click the **Save as CSV** toolbar icon to save your information as a CSV file. You can then use an application like Microsoft Excel* to import and work with the CSV file.

Changing query column headings

1. Open an existing query or create a new query.
2. In the bottom box, click a column heading and click **Edit**. Edit the heading and press **Enter**. Repeat as necessary.
3. Click **OK**.

Exporting and importing queries

You can export and import any queries you create. All queries export as XML files. If you export the same query filename more than once, it will overwrite the existing file. To avoid this, you may want to copy the file to another location once it's exported.

The export and import features are useful in two scenarios:

- If you need to reinstall your database, use the export/import features to save your existing queries for use in a new database.

For example, you could export the queries, then move them to a directory unaffected by a database reinstall. After reinstalling the database, you could move the queries back into the queries directory on your Web server, then import them into the new database.

- You can use the export/import features to copy queries to other databases.

For example, you could export a query to a queries directory on your Web server, then e-mail or FTP it to someone. That person could then place the queries into the queries directory on another Web server, then import them into a different database. You could also map a drive and directly copy queries into the queries directory on another Web server.

To export a query

Complete these steps while connected to a database that has a query you want to export.

1. In the left navigation pane, click **Queries**.
2. On the **Custom queries** page, click the query name you want to export. Click **Edit**.
3. On the **Edit query** page, click the **Export** toolbar button to export the query to disk.
4. On the **Query exported** page, right-click the query to download it as an XML file to a selected directory. The query becomes the XML file.

Note that If you export the same query filename more than once, it will overwrite the existing file. To avoid this, you may want to copy the file to another location once it's exported.

If you want to eventually import the query back into a database, you must move it to the queries directory recognized by the Web server, by default c:\inetpub\wwwroot\LANDesk\ldsm\queries.

To import a query

Complete these steps while connected to a database to which you want to import a query.

1. In the left navigation pane, click **Queries**.
2. On the **Custom queries** page, click **New**.
3. On the **Edit query** page, click the **Import** toolbar button.
4. Select the query you want to import. If you want to verify the parameters of this query before importing it, click **View**.
5. Click **Import** to load the query in the **Edit query** page.
6. Once the query is loaded, scroll down and click **Save query** to save it into this database.

LDAP queries

In addition to the ability to query the core database with database queries, you can also use the Directory manager tool that lets you locate, access, and target devices in other directories via LDAP (the Lightweight Directory Access Protocol).

You can query devices based on specific attributes such as processor type or OS. You can also query based on specific user attributes such as employee ID or department.

For information about creating and running database queries, see [Using database queries](#).

Read this chapter to learn about:

- About the Directory manager window
- Creating LDAP directory queries
- More about LDAP

About the Directory manager window

Use Directory manager to accomplish the following tasks:

- **New directory:** Opens the **Directory properties** dialog where you identify and log in to an LDAP directory.
- **Edit:** Edit the currently selected directory.
- **Delete:** Removes the selected directory from the preview pane and stops managing it.
- **Refresh:** Reloads the list of managed directories and targeted users.
- **LDAP targets:** Places selected LDAP objects in the target list.
- **New LDAP query:** Opens the **LDAP query** dialog where you can create and save an LDAP query.

The Directory manager window consists of three panes: a directory pane on the left, a preview pane on the right, and the bottom pane containing a target list and a list of LDAP queries.

Directory pane

The directory pane displays all registered directories and users. As an administrator, you can see a list of queries that are associated with the directory. You can create and then save new queries for a registered directory with a right mouse click or by using drop-down menus.

Creating LDAP directory queries

To create and save a directory query

The task of creating a query for a directory and saving that query is divided into two procedures:

To select an object in the LDAP directory and initiate a new query

1. In the left navigation pane, click **Directory manager**.
2. Browse the **Directory manager** directory pane, and select an object in the LDAP directory. You'll create an LDAP query that returns results from this point in the directory tree down.
3. From Directory manager, click the **New LDAP query** toolbar button. Note that this icon only appears when you select the root organization (o) of the directory tree (o=my company) or an organizational unit (ou=engineering) within the root organization. Otherwise, it's dimmed.
4. The basic **LDAP query** dialog appears.

To create, test, and save the query

1. From the basic **LDAP query** dialog, type a descriptive name in the **Name** field.
2. Click an attribute that will be a criterion for the query from the list of directory attributes (example = department).
3. Click a comparison operator for the query (=, <=, >=).
4. Enter a value for the attribute (example department = engineering).
5. To create a complex query that combines multiple attributes, select a combination operator (AND or OR) and repeat steps 1 through 3 as many times as you want.
6. When you finish creating the query, click **Insert**.
7. To test the completed query, click **Test query**.
8. To save the query, click **Save**. The saved query will appear by name under **Saved queries** in the directory pane of Directory manager.

About the basic LDAP query dialog

- **Name:** The name displayed in the directory pane.
- **LDAP query root:** Select a root object in the directory for this query (LDAP://ldap.xyzcompany.com/ou = America.o = xyzcompany). The query that you're creating will return results from this point in the tree down.
- **LDAP attributes:** Select attributes for user-type objects.
- **Operators:** Select the type of operation to perform relating to an LDAP object, its attributes, and attribute values including equal to (=), less than or equal to (<=), and greater than or equal to (>=).
- **Value:** Specify the value assigned to the attribute of an LDAP object.
- **Test:** Execute a test of the query you've created.
- **Save:** Save the created query by name.
- **Advanced:** Create a query using the elements of a basic LDAP query but in a freeform manner.
- **Insert:** Insert a line of query criteria.
- **Delete:** Delete a selected line of criteria.

About the Directory properties dialog

From the Directory manager toolbar, click the **New directory** toolbar button to open the **Directory properties** dialog. This dialog enables you to start managing a new directory, or to view properties of a currently managed directory. This dialog also shows the URL to the LDAP server and the authentication information required to connect to the LDAP directory:

- **Directory URL:** Enables you to specify the LDAP directory to be managed. An example of an LDAP directory and the correct syntax is `ldap.<companyname>.com`. For example, you might type `ldap.xyzcompany.com`.
- **Authentication:** Enables you to log into the directory. Specify a user name and password.

About the Advanced LDAP query dialog

From the **basic LDAP query** dialog, click **Advanced** to open the advanced **LDAP query** dialog, which displays the following:

- **LDAP query root:** Enables you to select a root object in the directory for this query. The query that you're creating will return results from this point in the tree down.
- **LDAP query:** Enables you to create a query using the elements of a basic LDAP query but in a freeform manner.
- **Example:** Displays query examples you can use as a guide when creating your own query in freeform.
- **Test query:** Enables you execute a test of the query you have created.

The Advanced **LDAP query** dialog appears when you select to edit a query that has already been created. Also, if you select an LDAP group in directory manager and then choose to create a query from that point, the Advanced **LDAP query** dialog appears with a default query that returns the users who are members of that group. You can't change the syntax of this default query, only save the query.

More about the Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for accessing and viewing information about users and devices. LDAP enables you to organize and store this information into a directory. An LDAP directory is dynamic in that it can be updated as necessary, and it is distributed, protecting it from a single point of failure. Common LDAP directories include Novell Directory Services* (NDS) and Microsoft Active Directory Services* (ADS).

The following examples show LDAP queries that can be used to search the directory:

- Get all entries: (objectClass=*)
- Get entries containing 'bob' somewhere in the common name: (cn=*bob*)
- Get entries with a common name greater than or equal to 'bob': (cn>='bob')
- Get all users with an e-mail attribute: (&(objectClass=user)(email=*))
- Get all user entries with an e-mail attribute and a surname equal to 'smith': (&(sn=smith)(objectClass=user)(email=*))
- Get all user entries with a common name that starts with 'andy', 'steve', or 'margaret': (&(objectClass=User) (| (cn=andy*)(cn=steve*)(cn=margaret*)))
- Get all entries without an e-mail attribute: (!(email=*))

The formal definition of the search filter is as follows (from RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> | <or> | <not> | <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> | <filter> <filterlist>
- <item> ::= <simple> | <present> | <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> | <approx> | <ge> | <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL | <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL | <value> '*' <starval>
- <final> ::= NULL | <value>

The token <attr> is a string representing an AttributeType. The token <value> is a string representing an AttributeValue whose format is defined by the underlying directory service.

If a <value> must contain one of the characters * or (or), precede the character with the slash (\) escape character.

Inventory management

Managing inventory

You can use the inventory scanning utility to add devices to the core database and to collect devices' hardware and software data. You can view, print, and export inventory data. You can also use it to define queries, group devices together, and generate specialized reports.

Read this section to learn about:

- Inventory scanning overview
- Viewing inventory data

Inventory scanning overview

When you configure a device with the device setup feature, the inventory scanner is one of the components that gets installed on the device. When creating a client configuration, you can specify when the inventory scanner runs on the device.

The inventory scanner runs automatically when the device is initially configured. The scanner executable is named LDISCAN32.EXE for Windows and LDISCAN for Linux. The inventory scanner collects hardware and software data and enters it into the core database. After that, the hardware scan runs each time the device is booted, but the software scan only runs at an interval you specify. To schedule a software scan, run SVCCFG.EXE in **Program Files | LANDesk | Management Suite**.

For more information on configuring the inventory service, see *Configuring the Inventory service* in Appendix C.

After the initial scan, the inventory scanner can be run from the console as a scheduled task. The standard LANDesk agent must be running on remote devices to schedule an inventory scan to them.

Note: A device added to the core database using the discovery feature has not yet scanned its inventory data into the core database. You must run an inventory scan on each device for full inventory data to appear for that device.

You can view inventory data and use it to:

- Customize the **All devices** list columns to display specific inventory attributes
- Query the core database for servers with specific inventory attributes
- Group devices together to expedite management tasks, such as software distribution
- Generate specialized reports based on inventory attributes
- Keep track of hardware and software changes on devices, and generate alerts or log file entries when such changes occur

Read the sections below to learn more about how the inventory scanner works.

Delta scanning

After the initial full scan is run on a device, subsequent running of the inventory scanner only captures delta changes and sends them to the core database. Use the scanner option /RSS to gather software information from the Windows registry.

Forcing a full scan

If you want to force a full scan of the device's hardware and software data, use the following method:

- Delete the INVDELTA.DAT file from the server. A copy of the latest inventory scan is stored locally as a hidden file named INVDELTA.DAT on the root of the hard drive. (The LDMS_LOCAL_DIR environment variable sets the location for this file.)
- Add the **/sync** option to the inventory scanner utility's command line. To edit the command line, right-click the **Inventory Scan** shortcut icon and select **Properties | Shortcut**, and then edit the **Target** path.

- On the core server, set the Do Delta registry key to 0. This key is located at: HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Do Delta

Scan compression

Inventory scans performed by the Windows inventory scanner (LDISCAN32.EXE) are compressed by default. The scanner compresses full scans and delta scans with approximately an 8:1 compression ratio. Scans are first built completely in memory, then compressed and sent to the core server using a larger packet size. Scan compression requires fewer packets and reduces bandwidth usage.

Scan encryption

Inventory scans are now encrypted (TCP/IP scans only). You can disable inventory scan encryption by setting the core server's Disable Encryption registry key to 0. This key is located at: HKLM\Software\Intel\LANDesk\LDWM\Server\Inventory Server\Disable Encryption

Viewing inventory data

Once a device has been scanned by the inventory scanner, you can view its system information in the console.

Device inventories are stored in the core database, and include hardware, device driver, software, memory, and environment information. You can use the inventory to help manage and configure devices, and to quickly identify system problems.

You can view inventory data in the following ways:

- Summary inventory
- Full inventory
- Viewing attribute properties
- System information

You can also view inventory data in reports that you generate. For more information, see Reports overview.

Viewing summary inventory from the local console

Summary inventory is found on the **Summary** page in the local console and provides a quick look at the device's basic OS configuration and system information.

Note: If you added a device to the core database using the discovery tool, its inventory data isn't yet scanned into the core database. You must run an inventory scan on the server for the summary inventory feature to complete successfully.

To view summary inventory

1. In the console's **All devices** view, double-click a device. Or single-click a device to select it and click **Launch local console** from the **Properties** tab.
2. In the left navigation pane, click **Summary**.

Windows 2000/2003 server summary data

This information appears when you view summary inventory for a Windows 2000/2003 server.

- **Health:** The current health state of the server.
- **Type:** The type of server, such as application, file, e-mail, and so forth.
- **Manufacturer:** The manufacturer of the server.
- **Model:** The server's model type.
- **BIOS version:** The version of the ROM BIOS.
- **Operating system:** Windows or Linux OS running on the server: 2000, 2003, or Red Hat.
- **OS Version:** Version number of the Windows 2000/2003 or Linux OS running on the server.
- **CPU:** Type of processor or processors running on the server.
- **Vulnerability scanner:** The version of the agent installed.
- **Remote control:** The version of the agent installed.
- **Software distribution:** The version of the agent installed.

- **Inventory scanner:** The version of the agent installed.
- **Last reboot:** The last time the server was rebooted.
- **CPU usage:** The percentage of the processor currently in use.
- **Physical memory used:** Amount of RAM available on the server.
- **Virtual memory used:** Amount of memory available to the server, including RAM and swap file memory.
- **Drive space used:** The percentage of drive space currently used. If you have more than one hard drive, each drive will be listed.

Servers that are IPMI-enabled display additional IPMI-specific data. Linux servers also display similar information in the **Summary** view.

Viewing a full inventory

A full inventory provides a complete listing of a device's detailed hardware and software components. The listing contains objects and object attributes.

To view a full inventory

1. In the console's **All devices** view, click a device.
2. In the **Properties** tab, click **View inventory**.

Viewing attribute properties

You can view attribute properties for a device's inventory objects from the inventory listing. Attribute properties tell you the characteristics and values for an inventory object. You can also create new custom attributes and edit user-defined attributes.

To view an attribute's properties, click the attribute in the left pane.

To print this information in Internet Explorer, right-click in the frame and click **Print**. To print in Mozilla, right-click in the frame, click **This Frame | Save Frame As**, click **Save**, then open the file in an application and click **Print**.

System information

From the local console, you can view and modify the device's system information. Information in the **Hardware**, **Software**, **OS event logs** and **Other** categories is either stored data or real-time data. When you click an information link you can view detailed information about the selected component and, in appropriate cases, set thresholds and enter information.

1. In the **All devices** list, double-click **My devices**.
2. In the console's **All devices** view, double-click a device. Or single-click a device to select it and click **Launch local console** from the **Properties** tab.
3. In the left navigation pane, click **System information**.
4. Click the information link you want to view.

Editing the LDAPPL3.TEMPLATE file

Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3.INI file to identify a device's software inventory. This file is placed on managed devices as part of agent configuration. Its parameters are set in the Inventory tab of Agent configuration.

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in the core server's LDLogon share.

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
Mode	<p>Determines how the scanner scans for software on devices. The default is Listed. Here are the settings:</p> <ul style="list-style-type: none"> • Listed: Records the files listed in LDAPPL3. • Unlisted: Records the names and dates of all files that have the extensions listed on the ScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network. • All: Discovers listed and unlisted files.
Duplicate	Records multiple instances of files. Set the value to OFF to record only the first instance, or ON to record all detected instances. The default is ON.
ScanExtensions	Sets the file extensions (.EXE, .COM, .CFG, etc.) that will be scanned. Use a space to separate the file extensions. By default, only .EXEs are scanned.
Version	The version number of the LDAPPL3 file.
Revision	The revision number of the LDAPPL3 file; helps ensure future compatibility.
CfgFiles 1-4	<p>Records the date, time, file size, and contents of the specified files. You can leave out the drive letter (for example, c:) if you want to search all local drives. You can specify more than one file on each of the four lines, but the line length is limited to 80 characters.</p> <p>Separate path names on the same line by a space.</p> <p>The scanner compares the date and size of the current file with that of the previous scan. If the date and size don't match, the scan records the contents of the file as a new revision.</p>
ExcludeDir 1-3	<p>Excludes specific directories from a scan. You can leave out the drive letter (for example, c:) if you want to exclude all local drives. Enumeration must start at 1 and be continuous. You must end each line with "\".</p>
MifPath	Specifies where MIF files are stored on a client's local drive. The default location is c:\DMI\DOS\MIFS.
UseDefaultVersion	If set to TRUE, the scanner reports a match when a file matches an exact filename and file size entry in LDAPPL3 on filename only (the version will be reported as EXISTS). This can cause some false positives for applications that share a common filename with an

unknown application. In the as-delivered LDAPPL3.TEMPLATE file, this parameter is set FALSE; that is, only add an entry if the match is exact. If the parameter is missing, it defaults to TRUE.

SendExtraFileData If set to TRUE, sends extra file data to the core server. The default is FALSE. This means that by default, only path, name, and version are entered into the core database.

To edit the LDAPPL3.TEMPLATE file

1. From your core server, go to the LDLogon directory and open LDAPPL3.TEMPLATE in Notepad or another text editor.
2. Scroll down to the parameter you're interested in updating and make your changes.
3. Save the file.

Updating the application list

The data from the applications list, DEFAULTS.XML, is stored on the core database. Because the names and version numbers of commonly-used software applications change fairly often, LANDesk publishes a new DEFAULTS.XML several times a year (in versions of LANDesk software before 8.6, this file was LDAPPL.INI).

To update the application list

1. Download a new DEFAULTS.XML or LDAPPL3.TEMPLATE file from <http://www.LANDesk.com/support/downloads>. Select a product and click **Software update** to download the file.
2. Save the file to the LDLOGON directory.
3. Publish a new LDAPPL3.INI by following the steps in Publishing the application list.

Publishing the application list

Publishing the Application list involves importing the most current application list in DEFAULTS.XML into the database, and then combining the application list with the contents of LDAPPL3.TEMPLATE to generate an updated LDAPPL3.INI file. There is a standalone utility COREDBUTIL.EXE in the Management Suite directory which is used to automatically perform both of these steps.

To publish the application list

1. Start CoreDBUtil.exe
2. Click the **Publish App List** button.

You should publish the application list after modifying or downloading an updated version of LDAPPL3.TEMPLATE or DEFAULTS.XML.

Software licenses

Monitoring software license compliance

IT administrators often find it challenging to track product licenses installed on numerous devices across a network. They run the risk not only of over-deploying product licenses, but also of purchasing too many licenses for products that turn out to be unnecessary. You can avoid these problems by using software license monitoring to monitor product licenses and usage across your organization.

The power of compliance monitoring rests in its data-gathering capabilities. Use the data to track overall license compliance and to monitor product usage and denial trends. The software monitoring agent passively monitors product usage on devices, using minimal network bandwidth. The agent continues to monitor usage for mobile devices that are disconnected from the network.

Monitoring features include:

- Ability to scan for both known and unknown applications.
- Application launch denial to keep unauthorized software from running even on devices disconnected from the network.
- Full integration with the Web console for current, complete information about installed applications.
- Extensive application usage and license compliance reporting.
- Extensive license monitoring and reporting features, including number of times each licensed application was launched, last date used, and total duration of application usage.
- Easy configuration of license parameters, including number purchased, license type, quantity and serial number.
- License purchase information, including price, date purchased, P.O. number, and reseller information.
- Installation tracking and reconciliation, including the license holder and physical location of the device the license is installed on, as well as additional notes.
- Aliases to track software when vendor information or filenames change.

How software license monitoring works

The software license monitoring agent, when installed, records the total minutes of usage, the number of launches and the last launch date of all installed applications on a device and stores this data in the device's registry at:

HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareMonitoring\MonitorLog

The device inventory scanner updates the core server with software license monitoring data when it does a software scan (by default, once a day). The inventory scanner uses a text file called LDAPPL3.INI to define which applications it should scan for. When the inventory scanner runs, it checks with the core server to see if the LDAPPL3.INI has been updated. If it has, the scanner gets the new version. The scanner uses file deltas and compression to minimize the amount of network traffic used. You shouldn't edit the LDAPPL3.INI file directly. For more information, see Publishing the application list.

Application usage data that you don't monitor is eventually overwritten with newer data in the device's registry.

About mobile devices

For mobile devices disconnected from the network, the Software Monitoring agent continues to record data and caches it in the device's registry. After the device reconnects to the network, the next scan detects which of the cached data is being monitored and sends that data to the core server.

Software license compliance tree

The software license monitoring tabs are designed to let you monitor and manage the software that's installed on your devices. Navigate to these tabs by clicking **Software licenses** in the left navigation pane.

Use the **Compliance** tree to monitor usage and license compliance for products across your organization, set up product license downgrading, deny usage of applications on devices, and view license compliance, usage, and denied application trends.

Use the **All products** tree to see all predefined products and products you created.

Creating product and vendor aliases

Use the **Aliases** tab to create product or vendor aliases. An alias ensures that you can correctly account for all installed products by:

- **Normalizing executable file data:** An alias lets you make consistent the information the core database needs to correctly identify an installed product. For example, the file information provided by a vendor isn't always consistent. Files scanned into the core database for various Microsoft products may show the vendor name as being Microsoft Corp, Microsoft (R), or just Microsoft. If you were to run a query on "Microsoft (R)" products, you would get only a partial list back of Microsoft products installed across your network. By creating a vendor alias of "Microsoft Corp" for all of your Microsoft products, you ensure that those products all have exactly the same vendor name.
- **Updating executable file data:** An alias lets you update file information if the product name or vendor changes after installation. For example, sometimes vendor or product names change because a company has been newly acquired or divested, or a company has renamed its product after several versions. If this occurs with your device applications, use aliasing to associate new vendor or product names with the originals, ensuring that the core database can continue to identify your executables accurately. This feature is especially useful if you're monitoring products in the Compliance tree and need to maintain accurate information about your licenses.

About the Aliases tab

The Aliases tab shows the original vendor and name for a product, as well as any new vendor and/or product names that you may have added. A software scan must occur before a new alias will appear in the compliance tree.

You can create two types of aliases:

- **Vendor:** An alias for all installed products of a certain vendor (enter the original vendor name and a new vendor name).

- **Product:** An alias for a specific product (enter original vendor and product names, as well as new ones). A product alias that includes a new vendor will always take precedence over an alias created for all products of a certain vendor.

To create an alias

1. From the left navigation pane, click **Software licenses**.
2. On the **Aliases** tab, click **New**.
3. Enter the original vendor and original product name, as well as the new vendor and/or new product name for the application. You must enter information for all alias fields, even if the original and new values are the same.
4. Click **OK**.

To edit an existing alias, click the alias and click **Edit**. To delete an alias, click the alias and click **Delete**. After you delete an alias, the database reverts to using the original vendor and product name after the next software scan.

Monitoring products for compliance

Setting up a product

The **Compliance** tree view contains a hierarchical tree of product groups and individual products. You can group products any way you want, for example:

- By company, such as Adobe* or Microsoft*
- By specific categories, such as Unauthorized Files or Accounting Department
- By product suite, such as Microsoft Office

Within these groups, add the products that you want to monitor for usage or denial trends. For example, under an Adobe group, you might add products such as Photoshop* and Illustrator*.

The **All products** tree view shows all predefined products and products you created. Drag products from this view into the compliance view so you can configure them for monitoring.

To set up a product

1. In the left navigation pane, click **Software licenses**.
2. If don't want to use an existing product group in the compliance tree, create one as described in Managing product groups. You can only add products to a group.
3. Click the group you want to create the product in. Click the **New** toolbar button.
4. Enter the product information, as described in Managing products.
5. Continue configuring the product by following the steps in Selecting product files to monitor.
6. Add license information by following the steps in Adding product license information.
7. Export the LDAPPL3.INI by following the steps in Customizing and exporting LDAPPL3.INI

Managing product groups

The **Compliance** tree view contains a hierarchical tree of product groups and individual products. You can group products any way you want, for example:

- By company, such as Adobe* or Microsoft*
- By specific categories, such as Unauthorized Files or Accounting Department
- By product suite, such as Microsoft Office

Within these groups, add the products that you want to monitor for usage or denial trends. For example, under an Adobe group, you might add products such as Photoshop* and Illustrator*. You can only add products to a group, and groups can't be nested.

To add product groups

From the left navigation pane, click **Monitor software**. In the **Compliance** tree view, do one of the following:

- To add a product group: Click the **Compliance** tree item, then click **New**. Enter the new group name and click **OK**.
- To edit a product group name: Click the **Compliance** tree item, and in the right pane click the group you want to edit. Click **Edit**. Enter the new group name and click **OK**.
- To delete or rename a product group or product: Click the **Compliance** tree item, and in the right pane click **Delete**. In the confirmation dialog, click **OK** to delete the group.

Managing products

You can add software license monitoring products under a product group. Create a new group or select an existing group for the product you want to add, as described in Managing product groups. Once you've clicked on a group and entered the product view, you can do the following:

- **Add a product:** Under the **Compliance** tree item, click the group you want to add the product to. Click the **New** button and select an existing product from the **Product list**, or enter a **Product name**.
- **Edit a product:** Under the **Compliance** tree item, click the group you want to edit a product in. In the right pane, click the product and click the **Edit** button. You can change the product name and check or clear the **Match all files** option.
- **Delete a product:** Under the **Compliance** tree item, click the group you want to delete a product in. In the right pane, click the product and click the **Delete product** button. When you delete a product it deletes the product from the tree view. Deleting a product doesn't remove files you specified as being part of the product from the main software file list.

The product dialog also allows you to choose the **Match all files** option. By default, the presence of any file in the **Product files** list will be considered a product match. The **Match all files** option requires all files be present on the client. For more information, see Tracking licenses using the match all files option.

Managing denied products

The denied products tree item doesn't allow groups. Instead, add, edit, and delete products at the root level. You can do this by clicking **Denied products** and then clicking the button that matches what you want to do. For more information on denied products, see Denying product execution.

Selecting product files

Use the a product's **Files** pane to specify which files should be monitored to determine when a product is running.


If you selected the **Match all files** option in the product properties dialog, all files you select must be on the device for software license monitoring to register a match. If you don't select the **Match all files** option, the presence of any file in the list on a device is considered a product match.

For denied products, the Match all files option is ignored. All files in a denied product will be blocked. For more information, see Denying product execution.

If you're tracking different products that use the same file, you need to treat the products sharing the file differently. For example, if you're tracking license usage for MSDE and SQL 2000, and they both use SQLSERVER.EXE of the same size, you should also track a .DLL or other application file that's unique to each product. The Web console won't monitor these other files for compliance (only executables are monitored for compliance), but the unique file will help the scanner distinguish the MSDE license from the SQL 2000 license.

If you add files to a product other than .EXEs, you must first edit the LDAPPL3.TEMPLATE file to include those files in a software scan. Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3.INI file to identify a device's software inventory. By default, LDAPPL3.INI only scans for executables. For more information, see Editing the LDAPPL3.TEMPLATE file.

To select files to monitor

1. In the left navigation pane, click **Software licenses**.
2. In the tree, click **Compliance | product group | product name | Files**. If you're working with a denied product file list, instead click **Denied products**.
3. Click the **Add** toolbar button.
4. In the **File** dialog, enter a filter string. You don't have to enter the full file name, and you can use an asterisk as a wildcard character.
5. Select the inventory column you want to search in, either Any, Vendor, Product name, File name, Version, or Size.
6. Select the file list you want to search in, either All, Discovered, or Not in product.
 - **All:** All predefined files in the LDAPPL3.INI (even if they haven't been discovered on devices), and all files that have been discovered on devices.
 - **Discovered:** Only files that have been discovered on devices, even if they're for products that aren't defined in the LDAPPL3.
 - **Not in product:** All files that aren't currently being monitored in the Compliance tree. Use this list to search for files that you may want to begin monitoring for license compliance and usage/denial trends. This view doesn't include files on the denied list.
7. Click the search button  beside the **In column** list to begin your search. Depending on the number of matches, it might take a while for the results to appear.
8. Click the files that indicate this product's presence on devices.

If the list of files spans multiple pages, use the arrows at the top of the page to navigate between pages. Enter the number of items to display per page and click **Set**.

Tracking licenses using the match all files option

Normally, software license monitoring considers the presence on a device of any file in the product's **Files** list of files a product match. You may encounter a situation where you need to track licenses for two or more products that contain an executable of the same name and size. In such a case, you also need to monitor a file unique to each product. By checking **Match all files** in the **Product dialog** and using both the executable and a unique file to identify license usage, you specify that all files associated with a product (as found in the **Product files** pane) need to be installed on a device before a product license is considered used. This ensures that the scanner can correctly track the products licenses.

The following two examples help explain when you would check **Match all files**:

- If you're tracking license usage for MSDE and SQL 2000, and they both use SQLSERVER.EXE of the same size, you should also track a .DLL or other application file that's unique to each product. The Web console won't monitor these other files for compliance (only executables are monitored for compliance), but the unique file will help the scanner distinguish the MSDE license from the SQL 2000 license.

If you add files to a product other than .EXEs (in order to use the Match All Files option), you must first edit the LDAPPL3.TEMPLATE file to include those files in a software scan. By default, LDAPPL3 only scans for executables. For more information, see Editing the LDAPPL3.TEMPLATE file.

- If you're monitoring 10 licenses for Office XP Standard (that includes Word, Excel, Outlook, and PowerPoint), as well as 10 licenses for Office XP Pro (that includes the same applications, in addition to Access), you face the problem of wanting to monitor two distinct product licenses that contain executables of the same name and size. The scanner can't distinguish between license types by tracking individual files, nor by using just the **Match all files** option for both products.

In this case, you must go one step further by adding an Office XP Pro executable to the **Product files** pane of XP Standard (for example, Access) and marking that executable as **Exclude from product**. This ensures that the software monitoring agent won't record an Office XP Pro license as an XP Standard license, which would occur if only **Match all files** was checked. For more information on marking a file as excluded, see Selecting product files to monitor.

Adding product license information

You must add license information to monitor a product for license compliance. If you only want to track product usage, you can skip this procedure.

After you set up license information for a product, if you ever see a red icon with an exclamation point appearing next to the product group, this means that one of the products in the group isn't license-compliant. Expand the product group to find the non-compliant product, then view its associated information in the right pane.

To add product license information

1. Click **Software licenses**.
2. In the **Compliance** tree, click **product group | product name | Licenses**.
3. Click the **New** toolbar button.
4. In the **License** dialog, enter the license, purchase, and tracking information that's relevant to your organization.

5. When finished, click **OK**.

To ensure that all executables associated with a product are installed on a device before that product's license is monitored for compliance, right-click the product name in the right pane and click **Edit product**. In the **Product** dialog, make sure **Match all files** is checked. For more information, see Tracking licenses using the match all files option.

About the License Properties dialog

The License Properties dialog has three tabs:

- License
- Purchase Info
- Tracking

Use the License tab to configure license properties for your product.

- **License number:** Enter a number that constitutes your product license.
- **License type:** Enter a type of license you have for the product, such as: competitive upgrade, freeware, new purchase, OEM, product upgrade, public domain, shareware, unknown.
- **Quantity:** Enter the number of product licenses purchased.
- **Serial number:** Enter an additional number that may constitute your product license.

Use the Purchase Info tab to configure purchase properties for your product license.

- **Purchase date:** Enter a date the product was purchased by your company.
- **Unit price:** Enter a price of each purchased license for the product.
- **Order number:** Enter an order number used to make the purchase.
- **Reseller:** Enter the name of purchase place.

Use the Tracking tab to configure tracking properties for your product license.

- **Owner:** Enter a person or department in your company responsible for storing the boxed product.
- **Location:** Enter a physical location where the boxed product is stored.
- **Notes:** Enter any additional information associated with the product license, such as downgrade rights.

Denying product execution

You can prevent devices from executing files you specify. When devices try to run a denied product, the product won't launch on their system and they'll see a message box telling them their system administrator has prevented access to that program.

You can restore normal access to a product by deleting the product in the **Denied products** group. Deleting a product here doesn't actually delete the product. It only removes the product from the group.

All files in **Product files** list for a denied product will be denied on devices. The **Match all files** product option state doesn't affect denied products.

You must publish the LDAPPL3.INI and devices must receive the updated version before changes take effect. For more information, see Publishing the application list.

Resetting usage data

If you ever want to clear the data for your monitored products' usage or denial reports, you can. Clearing the data lets you reset the counter so you can begin tracking applications from a certain point on. The reset affects all devices, and it clears the device registries and the core database of all past usage and denial report data. For this reason, it's important to print or save any usage or denial reports you may want to keep before resetting. When you reset the usage and denial report data, you do so for all monitored products in the Compliance tree.

To reset usage and denial report data

1. From the left navigation pane, click **Software licenses**.
2. In the lower pane, click the **Reset usage** tab.
3. Click **Next** to complete the reset.

After you reset, you'll need to force a scan to clear the report data from your device registries, then you'll have to force a second scan before the new data is actually recorded in the Software License Monitoring window.

On large databases, the reset can take a long time. If the reset times out, your DBA can reset the usage manually by entering these SQL commands:

```
UPDATE FileInfoInstance
SET SCM_TotalSessionTime = NULL,
SCM_SessionCount = NULL,
SCM_SessionsDenied = NULL,
SCM_LastUser = NULL,
SCM_LastSessionTime = NULL
```

Publishing the application list

The device inventory scanner uses an application list called LDAPPL3.INI that contains software inventory information. The LDAPPL3.INI is populated initially with most popular application executable filenames and file information. When the scanner runs on devices, it uses a local LDAPPL3.INI copy to match device executable filenames with the software inventory information.

The master LDAPPL3.INI resides in the core server's LDLogon share. Whenever you make a change to the application list, you must export a new LDAPPL3.INI file. When you export a new LDAPPL3.INI, the core server uses the LDLogon share's LDAPPL3.TEMPLATE text file to create the framework for the exported LDAPPL3.INI. The core server then populates this framework with file information from the core database. Finally, the core server writes the exported LDAPPL3.INI file to the LDLogon share, replacing any existing version. The next time servers do a software scan, they automatically receive the updated LDAPPL3.INI.

By default, LDAPPL3.INI contains descriptions of executables only. If you want the scanner to also identify other types of application files (.DLLs, .COMs, .SYSes, and so on), you can edit the LDAPPL3.TEMPLATE file to include all files of that type in a scan. For more information, see [Editing the LDAPPL3.TEMPLATE file](#).

You shouldn't edit the LDAPPL3.INI directly in a text editor, because the data is stored in the core server's core database. The next time the server writes a new version of this file, changes made directly with an editor will be lost. All changes to the LDAPPL3.INI should be made in the LDAPPL3.TEMPLATE file.

To publish a new application list

After changing the application list by editing the LDAPPL3.TEMPLATE file, publish a new LDAPPL3.INI by following the steps below.

1. From the left navigation pane, click **Software licenses**.
2. In the lower pane, click the **Publish list** tab.
3. Click **Next**.

Changes you make won't take effect on devices until they receive the updated LDAPPL3.INI.

Making the LDAPPL3.INI file available to devices

Each device that runs the inventory scanner has a local copy of LDAPPL3.INI. The devices' LDAPPL3.INI is initially installed as part of the default device configuration setup. Both the device and core version of this file must be synchronized for the scanner to know which files to scan or deny on devices. The core server and device LDAPPL3.INI synchronization uses delta matching so only the changes are transmitted. File compression further reduces the core's LDAPPL3.INI by 70 percent, which enables the scanner to update the devices' corresponding LDAPPL3.INI without using significant bandwidth.

If you don't want to wait for the next inventory scan to update your device LDAPPL3.INI files, you can make the edits available to devices by scheduling a job to push LDAPPL3.INI down to devices.

Using Asset Manager

LANDesk Asset Manager is a complete asset management solution that lets you record, track, and analyze any type of fixed asset within your organization—including IT assets like computers and monitors, office equipment, furniture, and any other valuable item you want to manage—in addition to critical business information such as contracts, invoices, and projects.

Asset Manager includes all the tools you need to configure data entry forms, enter items into the database with those forms, as well as collect and analyze that data with customizable reports.

For two of the predefined asset types, computers and software, Asset Manager also provides the capability to link and update asset data from the scanned inventory and SLM records.

Asset Manager is a Web-based application that runs in the LANDesk Web console. Note that Asset Manager is supported only in the Internet Explorer browser, and that Asset Manager is not accessible in the main Windows console.

Asset Manager 8 Add-On

Asset Manager is a separately purchased add-on product that integrates seamlessly with your current LANDesk network. If you haven't purchased or installed a LANDesk Asset Manager license, the user interface and the capabilities described here are not on your core server and will not be available from the Web console.

For information about purchasing an Asset Manager license, visit the LANDesk Web site.

For information about installing and activating the Asset Manager add-on product, refer to "Installing add-ons" in the *Installation and Deployment Guide*.

Read this chapter to learn about:

- Asset Manager overview
- Using role-based administration with Asset Manager
- Accessing Asset Manager in the Web console
- Managing assets
 - Working with computer assets
 - Working with software assets
- Managing contracts
- Managing invoices
- Managing projects
- Managing global lists
- Using subgroups to organize types
- Creating new types
 - Using a details summary
 - Adding details
 - Adding detail tables
 - Managing detail templates
 - Adding detail templates
 - Organizing details in sections
- Using an item list
- Adding items to the database
- Using asset alert dates
- Associating items
- Importing items
- Exporting items

- Searching for items
- Using Asset Manager reports

Asset Manager overview

Asset Manager adds easy-to-use features to the Web console that let you proactively manage all types of fixed (non-scannable) assets across your enterprise throughout the entire asset life cycle. In addition to physical assets, you can manage other relevant information such as contracts, invoices, and projects. If implemented and maintained properly, this type of information management can provide the security, access, and control of important data necessary to not only make informed business decisions and planning, but improve the productivity and efficiency of your organization's everyday business operations.

In short, Asset Manager helps you get the most out of your IT investments.

Linked data from the core database (for computers and software)

With Asset Manager, you can leverage existing data for computers and licensed software products that has already been scanned (via the inventory scanner) or entered manually into your core database.

Import and export capabilities

You can also use Asset Manager to import and export asset data to use with other data tracking and management applications and databases. The import and export features support both CSV (comma-separated value) and XML formatted files.

Other features and benefits

In addition to the features mentioned above, with Asset Manager you can:

- Use predefined types (i.e., data entry forms) or create your own custom types that are used to add items to the database.
- Store asset management data in a single repository—the core database. A single database simplifies data management, ensures data accuracy and integrity, and allows multiple users to enter asset data and generate reports at the same time.
- Associate assets with each other and with other related information, such as invoices, users, service histories, etc.
- Set up alert dates to automatically notify you when an asset's pre-established deadline expires.
- Use predefined asset management reports or create your own custom reports.
- Reconcile recorded asset data with actual physical inventories.
- Track asset data history.

Understanding Asset Manager types and details

Asset Manager uses types and details to describe the kinds of items (and their inherent properties) that can be added into the database. A *type* simply represents a specific kind of asset, contract, invoice, project; and so on. And a *detail* represents specific information about that type. To understand this concept in practical terms, it's probably helpful to think of a type as essentially a data entry form (made up of details) for a particular kind of item, and each detail as an individual data field on the form.

Asset Manager has several predefined asset types, contract types, invoice types, project types, and global list (or universally applicable) types, each defined by its own unique combination and arrangement of details. However, you're not limited to these types or details. With Asset Manager, you can also create and modify your own custom types, details, detail tables, and detail templates in order to meet your asset management requirements and goals. You're able to determine the content and layout of a data entry form, what type of information is being asked for, whether a data field is required, and more.

Ultimately, the purpose of asset types and details is to give you a way to configure data entry forms that you then fill out in order to add items to the database.

Asset management workflow

The following steps provide a quick summary outline of the typical processes involved in implementing an asset management strategy on your LANDesk network. Each of these tasks is described in detail in the appropriate sections of this chapter.

1. Managing types (viewing, organizing, editing, and deleting) with the Assets, Contracts, Invoices, Projects, and Global Lists pages.
2. Creating types (i.e., data entry forms) with the Add new type page.
3. Creating details (i.e., data fields) for types with the Add details page. Also, adding detail tables and detail templates to types.
4. Adding items to the database by filling out data entry forms.
5. Importing and exporting asset items.
6. Using predefined and custom reports to collect and analyze asset data.

Using role-based administration with Asset Manager

Role-based administration is LANDesk's access and security model that lets LANDesk Administrators restrict access to tools and devices. Each user is assigned specific rights and scope that determine which features they can use and which devices they can manage. For more information about role-based administration, see *Using role-based administration in the Users Guide*.

Role-based administration can also be implemented to control access to features in the Web console, including the Asset Manager tool. To learn more about how role-based administration works for the basic Web console interface and tools, see *Using the Web console in the Users Guide*.

Asset Manager introduces three new roles and corresponding rights to role-based administration. An administrator assigns these rights to other users with the Users tool in the main console (see the *Users Guide* for details). In order to see and use the various Asset Manager features in the Web console, a user must be assigned the necessary Asset Manager right, as described below.

Note: In addition to users that have only one of the rights below, a user could have both the Asset Data Entry and Reports rights. Since Asset Configuration gives full access to Asset Management, any combination with it would be redundant.

Asset Configuration

The Asset Configuration is an administration-level right that provides users the ability to:

- See and access all the Asset Management links in the Web console: Assets, Contracts, Invoices, Projects, Global Lists, Detail Templates, and Reports.

- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

Asset Data Entry

The Asset Data Entry right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global Lists links in the Web console.
- Browse types and details (can't add, edit or delete them)
- Add items to the database by filling in data entry forms
- Edit items that have been added to the database

Reports

The Reports right for asset management-specific reports is the same Reports right that allows users to generate and view all other reports in the main console. This right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, Global Lists, and Reports links in the Web console.
- Browse types, details, and items (can't add, edit or delete them)
- Run predefined Asset Manager reports
- Create and run custom asset reports
- Edit all report configurations
- Print all reports

Accessing Asset Manager in the Web console

Asset Manager is a browser-based application that is accessed through the Web console (note that Asset Manager is supported only in the Internet Explorer browser). Asset Manager features and interface do not appear at all in the main Windows-based console. In order to use Asset Manager, you must already have the Web console software installed on either your core server or on another Web server on your network.

For more information about the Web console

For information on installation prerequisites and procedures for the Web console, see Installing the Web console in the *Installation and Deployment Guide*.

For more information on logging in to the Web console and using the default Web console features, see Using the Web console in the *Users Guide*.

Users with a valid Web console account can access Asset Manager in the Web console from any Windows-based computer running Internet Explorer 5.5 or later.

To access Asset Manager in the Web console

1. From a networked computer, open Internet Explorer.
2. In the Address field, enter the URL to the site hosting the Web console pages. Normally the URL is: `http://webservername/remote`.
3. Once you authenticate, an Asset Manager link appears in the left navigation pane. Clicking on this link will open Asset Manager in its own browser window, with features displayed based on the user's role based administration rights.

What's next?

Now that you have a basic understanding of what you can do with Asset Manager and have logged into the Web console, you can click any of the Asset Management links and start using the features introduced in this overview section.

Online help

From any page in the Web console, including Asset Manager pages, click the Online Guide link in the upper right corner to access online context-sensitive help for that page.

Managing assets

The Assets page shows all the asset groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Assets are defined as IT items or property that can't be scanned by the inventory scanner into the core database but that you want to track and manage, such as printers, monitors, phones, desks, supplies, etc. The exception to this definition are the computer and software types (see below for an explanation about these two special asset types). There's no limit to the number or variety of IT assets you can record with Asset Manager.

Asset *types* represent the data entry forms used to enter asset items into the database. You can use the predefined asset types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the **Add Type** link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) **Add** link and filling out the data entry form.

The predefined asset groups and types include:

Miscellaneous

- Chair
- User

Office Equipment

- Copier
- Digital Camera
- Fax
- Mobile Phone
- Phone
- Projector
- Television

Technology

- Computer
Important: Computer is a special asset type because it contains linked data that can be updated and synchronized with inventory data in the core database. The computer asset type can't be deleted or renamed. For more information, see [Working with computer assets](#).
- Monitor
- PDA
- Printer
- Router
- Scanner
- Software
Important: Software is a special asset type because it contains linked data that can be updated and synchronized with inventory data. The software asset type can't be deleted or renamed. For more information, see [Working with software assets](#).
- Switch

Working with computer assets

The computer type is one of two asset types with linked details (data fields) that can be updated and synchronized with information from the core database. Designated computer type details are linked to a scanned device's hardware inventory (a scanned or managed device is one on which the Management Suite inventory scanner has been run). The other asset type with linked details that can be updated with information from the core database is the software type.

You can use linked details to populate linked data fields for computers that have already been scanned and have an inventory record. For computers that aren't yet connected to your network or haven't yet been scanned by the inventory scanner, you can manually add computer items in Asset Manager (using a valid MAC addresses or serial number provided by the manufacturer), and populate the other linked data fields after the machines have been scanned.

The computer asset type can't be deleted or renamed.

Linked details for computers

Only designated computer details are linked and can be updated from a scanned computer's hardware inventory. These details are identified by the linked-chain icon. Linked details can't be deleted, and you can't create your own linked details.

The following computer details are linked:

- Device ID

Important: The Device ID linked detail can be thought of as the master link because it is used to definitively identify each specific computer asset in the hardware inventory, ensure there are no duplicate records, and synchronize the appropriate linked data for each computer asset. Device ID is listed as a Hidden information type in the computer details summary page, and only its Default value and Summary fields can be edited manually.

- Machine name
- Manufacturer
- MAC address
- Serial number
- Model
- Asset tag
- Domain name
- Description
- Notes
- Last hardware scan date
- Primary owner (the user who has logged in to a device the most times within a specified number of logins. The default number of logins is 5.)

All other details for the computer type are not linked and must be entered and updated manually.

You can manually enter information in linked data fields only BEFORE updating those details with inventory information. Once a computer's linked data has been updated, the linked data fields can no longer be edited manually. However, you can refresh/update linked data from the inventory as many times as you like.

Non-linked data fields can always be edited in Asset Manager. Non-linked data does not appear in a scanned device's inventory tree.

Updating linked data for computers

You can update all of your scanned computers at once from the computer item list page (this may take a long time depending on how many managed devices you have in the core database). Or, you can update linked data for an individual computer from its own page.

Asset inventory update utility

You can also update both computer and software asset data at the same time with a utility executable installed on the core server by the Asset Manager setup program. You can use this utility to update asset data manually or as a scheduled task with Windows Task Scheduler. For more information, see [Using the asset inventory update utility](#).

To update the computer item list

1. From the Assets page, open the **Technology** subgroup, and then click **Computer** to view all the computer assets currently recorded in the database.
2. Click the **Refresh asset data** link located above the computers list.

Scanned devices that do not have a corresponding computer item on this page are added to the list, with their linked data fields filled in. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

If a corresponding computer item already exists on this page, its linked data is refreshed/updated from the scanned device's inventory. If the information has changed in the inventory, the new information replaces the value in the linked data field. Only linked data fields are updated.

To update linked data for one computer item

1. From the computer item list page, edit the computer by clicking its pencil icon.
2. Click the **Refresh asset data** link located above the details list.

The computer's linked data is updated with information from the corresponding scanned device's inventory. This process rewrites any manually entered or changed value in a linked data field with the current value in the inventory. Empty linked data fields are filled in, if that data exists. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

From a specific computer's page, you can also click the **Open inventory data** link located above the details list to view the scanned device's entire inventory tree.

Note: If the Open inventory data option is not available on a computer's page, it indicates the corresponding device has been deleted from the hardware inventory. When a device is deleted from the inventory, its asset record is not removed from Asset Manager.

Using the asset inventory update utility

When you install the Asset Manager add-on, an utility executable is copied to the LDMain folder on the core server (the LANDesk\ManagementSuite folder). This utility provides the convenience of being able to refresh all of the computer and software license asset data that currently resides in the core database at once, either manually or as a scheduled task at a specific time. In other words, you don't have to perform this task via the computer or software item list pages in the Web console's Asset Manager pages.

The name of the executable file is:
LANDesk.ManagementSuite.AssetManagement.InventoryUpdate.exe

You can run this utility by any of the following methods:

- Double-click the executable file
- Run the executable from a command line interface
- Create a Windows Scheduled Task that runs this executable. Note this is NOT a LANDesk Scheduled Task.

To create a Windows Scheduled Task to update (refresh) computer and software asset data

1. At the core server, click **Start | Programs | Accessories | System Tools | Scheduled Tasks**.
2. Click **Add Scheduled Task** to open the Scheduled Task wizard, and then click **Next**.
3. Use the **Browse** button to locate and select the utility executable (named above) in the ManagementSuite folder, and then click **Next**.
4. Enter a name for the task, select the frequency when the task should be performed, and then click **Next**.
5. If necessary, select the time and day when the task should be performed, and then click **Next**.
6. Enter the user name and password for a valid LANDesk Administrator user, and then click **Next**.
7. Click **Finish**. The task should appear in the Scheduled Tasks window. (You can right-click a task to run it, delete or rename it, or to modify any of the task's basic or advanced settings.)

Working with software assets

The software type is one of two asset types with linked details (data fields) that can be updated and synchronized with information from the core database. Designated software type details are linked to license file information for your licensed software products. The other asset type with linked details that can be updated with data from the core database is the computer type.

You can use linked details to populate linked data fields for software that has a license file recorded in Software License Monitoring (SLM) in the main console or in the Compliance section in the Web console. For more information about the SLM tool, refer to the *Users Guide*.

The software asset type can't be deleted or renamed.

Linked details for software

Only designated software details are linked and can be updated from SLM. These details are identified by the linked detail icon. Linked details can't be deleted, and you can't create your own linked details.

The following software details are linked:

- Product name
- Version
- Publisher
- Product Link ID

Important: The Product Link ID linked detail can be thought of as the master link because it is used to definitively identify each specific software asset in SLM, ensure there are no duplicate records, and synchronize the appropriate linked data for each software asset. Product Link ID is listed as a Hidden information type in the software details summary page, and only its Default value and Summary fields can be edited manually.

- License number
- License type
- Quantity
- Serial number
- Purchase date
- Unit price
- Order number
- Reseller
- Owner
- Location
- Note

All other details for the software type are not linked and must be entered and updated manually.

You can manually enter information in linked data fields only BEFORE updating those details with SLM information. Once a software product's linked data has been updated, the linked data fields can no longer be edited manually. However, you can refresh/update linked data from the product information in SLM as many times as you like.

Non-linked data fields can always be edited in Asset Manager.

Updating linked data for software

You can update all of your software products that have a valid license file at once from the software item list page. Note that not all of your licensed software products in SLM necessarily have a license file. Only those licensed products with an actual license file will be updated. Or, you can update linked data for an individual software product (that has a license file) from its own page.

Asset inventory update utility

You can also update both computer and software asset data at the same time with a utility executable installed on the core server by the Asset Manager setup program. You can use this utility to update asset data manually or as a scheduled task with Windows Task Scheduler. For more information, see Using the asset inventory update utility.

To update the software item list

1. From the Assets page, open the Technology subgroup, and then click **Software** to view all the software assets currently recorded in the database.
2. Click **Refresh asset data** link located above the

Software products (with a license file) that do not already have a corresponding software item on this page are added to the list, with their linked data fields filled in. If there is no data the field is left blank, and can't be edited.

If a corresponding software item already exists on this page, its linked data is refreshed/updated from the license file information in SLM. If the information has changed in SLM, the new information replaces the value in the linked data field. Only linked data fields are updated. If there is no data the field is left blank, and can't be edited.

To update linked data for one software item

1. From the software item list page, edit the software product by clicking its pencil icon.
2. Click **Refresh asset data** link located above the details list.

The software product's linked data is updated with information from the corresponding product's license file information in SLM. This process rewrites any manually entered or changed value in a linked data field with the current value in SLM. Empty linked data fields are filled in, if that data exists. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

Managing contracts

The Contracts page shows all the contract groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Contracts can be any sort of document pertaining to the formal business relationships you have with service providers, partners, and vendors that you want to record and manage. Record critical information about the contract such as names, effective dates, status, contract numbers, terms and conditions, relationships, etc., and then associate the contract with the assets it covers. For example, you could enter data about a lease agreement for a group of printers, and then associate the lease with the printers.

Adding contract information to the database not only helps you keep track of valuable assets but also the important information you need for negotiating terms and conditions for future contracts.

Contract *types* represent the data entry forms used to enter contract items into the database. You can use the predefined contract types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined contract groups and types include:

Standard

- Consulting Agreement
- Escrow
- Lease

Managing invoices

The Invoices page shows all the invoice groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Invoices are documents pertaining to the purchase, acquisition, or payment of products and services. With Asset Manager, you can enter and store relevant information about an invoice and associate it to the corresponding asset.

Invoice *types* represent the data entry forms used to enter invoice items into the database. You can use the predefined invoice types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined invoice groups and types include:

Standard

- Invoice
- Purchase Order

Managing projects

The Projects page shows all the project groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Large, complex projects typically involve the purchase and use of a variety assets and related materials. With Asset Manager, you can enter specific project information into the database, associate the project with any other recorded item, and then generate custom reports to help you track and manage the project.

Project *types* represent the data entry forms used to enter project items into the database. You can use the predefined project types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined project groups and types include:

Miscellaneous

- Ad hoc

Standard

- Capital Expenditure
- Sustaining

Managing global lists

The Global Lists page shows all the global list groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Global lists refer to lists of standard information, such as locations, companies, and users, that can be applied globally to describe assets throughout your organization. By defining these global lists in one place, and using them to add standard data to other types, you can ensure consistent usage in all your asset management records. For example, if you need to update data in a global list, such as a department's name or company's address, the new information propagates automatically to all other items that include that standard global list data.

Global List *types* represent the data entry forms used to enter global list information into the database. You can use the predefined global list types and create your own custom global list types.

On a data entry form, an Expand/Collapse icon next to a data field's text box identifies it as a global list type that can be used to select a detail from a list of that global list type's available details. Whereas, an Expand/Collapse icon next to a data field name, where there is no text box, identifies a table detail.

Using global lists to add a detail to a type

Global lists are different from the asset, contract, invoice, and project types because you can use a global list type to add a standard detail (or data field) to any of the other types. For example, let's say you're adding a detail to a new asset type; choosing "Global List" opens a new dialog where you can select the global list type called "locations" (and, if you want to specify a default value, you can also select a specific location from the drop-down list of available locations). In this way, global list types are truly global, meaning they're available for all other types, and provide standard, consistent information across the database's asset records.

As previously mentioned, if a detail in a global list type is changed, the change is reflected in any recorded item that uses that detail.

Using global lists to organize and view types

Global lists serve another unique purpose in Asset Manager. They can be used as parent groups to view lists of asset, contract, invoice, and project types. From any of the type pages, you can click the **Group by** drop-down list and select a global list (predefined and custom) by which to arrange the types on that page.

For example, if you want to view computer asset types by location, select the "location" global list. Each current location appears as a parent group that can be expanded to show the types (in their subgroups) with matching location data. Types that do not contain location data are listed under the "No Information" parent group. If there aren't any types in the "location" global list type, the "No Information" parent group displays, containing all the page's subgroups and types.

If you select **None** from the Group by menu, subgroups and types are listed without a parent global list group. None is the default setting.

As with other type pages, from the Global Lists page you can:

- View types in subgroups. (Grouping by global list types is not supported on the global lists page.)
- Create, edit, and delete subgroups by clicking the Manage subgroups link.

- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined global list groups and types include:

Default

- Company
- Cost Center
- Department
- Location
- Vendor

Displaying large global lists

The more items you place in a global list, the longer it takes for a page containing that global list to display. For example, when a global list is included in a specific type's definition, that type's Add Items and Edit Items data entry pages take longer to display. Also, selecting a global list that contains a large number of items in the Group By drop-down list may take longer to display.

Creating new types

Use the Add new type page to create your own custom types for assets, contracts, invoices, projects, and global lists.

As a reminder, it might be helpful to consider types as data entry forms comprised of specific details that define an item. Types are divided into the following five major categories in order to facilitate tracking and reporting: Assets, Contracts, Invoices, Projects, and Global Lists. For example, a printer is an asset type, a lease is a contract type, and a location is a global (i.e., generally applicable) type. To continue the example, a printer asset type could be comprised of details (data fields) specifying the printer's manufacturer, model, description, service history, warranty type, cost, and so on. A type is used to add items to the database.

Asset Manager comes with several predefined types that can be used to add common items to the database. You also have the flexibility to create as many additional custom types as you like to accommodate all of the IT assets and critical information you want to manage.

The first step in creating a new type is to define the type's key detail. After the key detail is defined you can add as many other details as you like. All types are created by the same procedure, described below.

To create a new type

1. From any Asset Manager type page (Assets, Contracts, Invoices, Projects, Global Lists), click the **Add type** link next to the group where you want to add the type.
2. In the **Type name** field, enter a unique name for the type.
3. In the **Key name** field, enter a name for the key detail. Every type must have one (and only one) detail designated as the "key" so that it can be tracked in the database. When you initially create a new type, you're required to specify the name of its key detail. If the key detail is the only detail for a type, it must also be a unique and required value.

Once a type is created you can't delete its key detail. Additionally, once designated you can't change a type's key detail to be another detail.

4. From the **Type** drop-down list, select the type of information you want this type's key detail to represent. Available kinds of information include: String (alphanumeric characters or symbols), Integer (whole number), Date (calendar date), Decimal (real number that allows two decimal places; the decimal point separator can be either a period or a comma), and Alert Date (calendar date; for more information, see Using asset alert dates).

Note: Static List and Global List are not valid information types for the key detail. However, they can be used when creating additional details. For more information, see Adding details.

5. If you selected the String type, you must specify the maximum number of characters allowed in the string by entering a numerical value in the **Length** field. The valid range is from 1 to 4,000 characters for English and other European languages (the range is from 1 to 2,000 characters for supported double-byte Asian languages). This field is required for a string and is not available for any other information type.
6. Again, if you selected the String type, you can enter a required format or syntax in the **Input Mask** field. This field only applies to strings and is optional.

The input mask indicates a required format when entering data for this detail on a data entry form. For example, if the detail is a serial number that must conform to a certain format such as "abc-123456" you would enter an input mask like this: aaa-#####, where lower-case "a" represents any letter, the hyphen is a literal character, and the pound character (#) represents a number. For the actual character a, use the /a exception. For the actual pound character (#), use the /# exception. This mask appears on the data entry form so the user knows how to enter data for the field.

Note: Only the alphanumeric characters a-z, A-Z, and 0-9 are supported when filling in a string detail on a data entry form whose required syntax is specified by an input mask. Extended characters and double-byte characters are NOT supported.

7. If you want to specify a value that will automatically appear in the key detail's data field on a data entry form, enter that value in the **Default Value** field. You can enter a default value for any type of information. This field is optional. (To enter a default date value, use the calendar control.)

Note: Any default value specified here can be changed when filling out the actual data entry form.

8. Click **Save** to save the type and its key detail, and to return to the Details for... page.

At this page you can continue to configure the type by adding more details, detail tables, or detail templates. You can also change the subgroup where this type resides with the **Belongs to** drop-down list.

9. **Important:** When you're done configuring the type, you must also click **Save Details** on the Details for... page in order to save all the details you've added to that type.

Once a custom type is created, you can:

- Edit a type's details by clicking the pencil icon.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Add items to the database by clicking the plus sign (+) **Add** link and filling out the data entry form.

Using a details summary

This page provides a summary view of all the details that make up the type named at the top of the page. A type's details are what appear on a data entry form for that type.

Each type's details summary page is unique, depending on the details that have been used to define that type. However, the tasks you can perform from any details summary page are the same.

From any details summary page, you can:

- View all the details that define the selected type.
- Edit existing details by clicking the pencil icon next to the detail name.
- Create new details for a type by clicking the Add detail link.
- Create an alert date detail for a type.
- Add a group of details to a type at once by clicking the Choose template link.
- Add a table data field to a type by clicking the Add table link.
- Delete a detail by clicking the X icon.
- Organize details in configurable sections by clicking the Manage sections link.

Important note on saving changes to details:

In order to preserve any changes you've made to details in the details summary list (including changes to detail templates and detail tables), you must always click **Save Details** on this page. If you add, modify, or delete one or more details and then click **Cancel** on this page, none of your changes will be saved.

Understanding the detail icons

The details summary page includes a legend with icons that indicate different characteristics for the detail. Detail icons appear here in a details summary list, as well as on an item page and on data entry forms next to data fields.

The legend shows the following icons:

Key: Indicates the detail is the key identifying detail for this type. Each type must have one, and only one, key detail in order to be saved. Key details are automatically unique and required. A key detail can't be deleted or changed.

Unique: Indicates the detail must have a unique value entered when filling out the data entry form. If you enter a duplicate entry (the same value already exists in that data field for another item), an error message displays. Unique details are automatically required. Types can have multiple details that ask for unique data.

Required: Indicates the detail must have valid data entered when filling out the data entry form. A required detail may or may not be unique. For example, if a detail is marked required but not unique, you can enter the same data in that field on data entry forms for different items.

Summary: Indicates the detail will appear as a column heading on an item list page.

Linked: (Applies only to the computer and software asset types) Indicates the detail is linked to corresponding scanned device data, or entered software license data, in the core database. The linked characteristic applies to only some of the details for the computer and software asset types, not all of their details. The linked characteristic does not apply to any details for any other asset type. You can't create your own linked details.

Asset Manager lets you update and synchronize linked data by using the computer or software asset's Refresh feature. Computer assets are updated with the current device inventory data that has been scanned into the core database by the inventory scanner. Software assets are updated with the licensed software products data you've entered into the core database.

Adding details

Use this page to add a new detail, or edit an existing detail, for an asset type.

Details represent the data fields on an item's data entry form. When you fill out a data entry form, that item is added to the core database and can be tracked and managed with Asset Manager.

To edit an existing detail, click the pencil icon next to the detail name. For a description of what information you can and can't edit on a saved detail, see Rules for editing details below.

To add a new detail

1. From any details summary page, click the **Add detail** link.
2. In the **Name** field, enter a unique name for the detail.
3. From the **Type** drop-down list, select the type of information you want this detail to represent. Available kinds of information include: String (alphanumeric characters or symbols), Integer (whole number), Date (calendar date), Decimal (real number that allows two decimal places; the decimal point separator can be either a period or a comma), Alert Date (calendar date; for more information, see Using asset alert dates), Static List (lets you create a predefined list of values; see the Static List step below), and Global List (lets you select any of the current global list types; see the Global List step below).
4. The **Key** option is not available because this is not the initial detail. The key detail is defined when you initially create the type, and it can't be changed or removed.
5. Select the **Unique** option if you want to indicate on the data entry form that this detail (data field on the form) needs to be filled in with a unique value. In other words, duplicate entries among recorded items won't be allowed in this data field.

If you select the Unique option, the Required option (below) is automatically selected as well. This is because a data field that asks for a unique value is considered a required field by default.

6. Select the **Required** option if you want to indicate on the data entry form that this detail (data field) must be filled in with valid data. A required field is indicated by the red "i" icon on a data entry form. A required data field does not necessarily have to be filled in with unique data.
7. If you selected the String type, you must specify the maximum number of characters allowed in the string by entering a numerical value in the **Length** field. The valid range is from 1 to 4,000 characters for English and other European languages (the range is from 1 to 2,000 characters for supported double-byte Asian languages). This field is required for a string and is not available for any other information type.
8. Again, if you selected the String type, you can enter a required format or syntax in the **Input Mask** field. This field only applies to strings and is optional.

The input mask indicates a required format when entering data for this detail on a data entry form. For example, if the detail is a serial number that must conform to a certain format such as "abc-123456" you would enter an input mask like this: aaa-#####, where lower-case "a" represents any letter, the hyphen is a literal character, and the pound character (#) represents a number. For the actual character a, use the /a exception. For the actual pound character (#), use the /# exception. This mask appears on the data entry form so the user knows how to enter data for the field.

Note: Only the alphanumeric characters a-z, A-Z, and 0-9 are supported when filling in a string detail on a data entry form whose required syntax is specified by an input mask; extended characters and double-byte characters are not supported.

9. If you want to specify a value that will automatically appear in this detail's data field on a data entry form, enter that value in the **Default Value** field. This option applies to all the information types and is not required. All default values on a form can be edited. (To enter a default date value, use the calendar control.)
10. If you want this detail to appear on the item list page for the type you're configuring, select the **Summary** option. This option is checked by default. If you clear the Summary option, this detail does not appear on the item's list page.
11. If you want to configure a controlled list of valid data entry values for this detail, select **Static List** type. A new dialog appears to the right that lets you add values to the static list. The values you add to this list will be available for this detail in a drop-down list on the data entry form.

To add values to the static list, simply enter a value in the **Add Values** text box and click the plus sign (+). To set a value as the default value (automatically appears in the detail's data field on a data entry form), select the value and then click **Set Default**. To remove a value, select it and click **Remove**.

12. If you want to use a global list type to define this detail, select **Global List** type. A new dialog appears to the right that lets you choose from the current global list types (see Managing global lists). The values that have been added to the database for the selected type will be available for this detail in a drop-down list on the data entry form.

Global lists contain general information that is standard throughout your organization, such as vendors, users, and locations. To use a global list type to define this detail, first select the subgroup that includes the global list type you want from the **Select Group** drop-down list, and then select the global list type from the **Select Type** drop-down list. (If you want to assign a default value to this detail (data field on the form), select a value from the **Select Default Value** drop-down list. Keep in mind that if no data has been entered into the database for that type yet, this list will be empty.)

13. When you're done configuring the settings and values for the detail, click **Return to form** to save the detail and return to the details summary page. Or, click **Cancel** to exit without saving the detail.
14. If you want to place the detail in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see Organizing details in sections.
15. **Important:** You must also click **Save Details** on the details summary page to save any details you've added or modified.

Rules for editing details

After a type has been saved, you can edit only some of the information fields for the details that define that type.

Remember that a type must have at least one detail, called the key detail. In addition to its key detail, a type can have any number of additional details that help define that type and help you track and manage your IT assets.

Non-editable fields

For both key and non-key details, AFTER the detail is saved you can't edit any of the following information fields on the Edit Detail page:

- Name
- Type
- Key
- Unique
- Required

Editable fields

Whether the other information fields can be edited is different for key and non-key details, as described below.

For key details:

For a key detail, the table below shows the fields on the Edit Detail page that can be edited, depending on the selected information type:

Information Type	Length	Input Mask	Default Value	Summary
String	Yes	Yes	Yes	No
Integer	No	No	Yes	No
Date	No	No	Yes	No
Decimal	No	No	Yes	No
Alert Date	No	No	Yes	No

For non-key details:

For a non-key detail, the table below shows the fields on the Edit Detail page that can be edited, depending on the selected information type:

Information Type	Length	Input Mask	Default Value	Summary	Static List Values	Global List Default Value
Integer	No	No	Yes	Yes	No	No
String	Yes	Yes	Yes	Yes	No	No
Date	No	No	Yes	Yes	No	No
Decimal	No	No	Yes	Yes	No	No
Alert Date	No	No	Yes	Yes	No	No
Static List	No	No	Yes	Yes	Yes	No
Global List	No	No	No	Yes	No	Yes

Adding detail tables

Use this page to add a detail table to the selected type. A detail table consists of one or more details and appears as an expandable table data field on a data entry form, each detail represented by a separate column in the table.

On a data entry form, an Expand/Collapse icon next to a data field name (without a text box) identifies a detail table. In contrast, an Expand/Collapse icon next to a data field with a text box identifies a global list type.

One example of a table data field on a form is a service history table, that consists of details such as cost, service date, technician, vendor, and so on.

When filling in a form, users can add as many entries as they like into a table data field by clicking the **Expand** icon, clicking the **Add** link, filling in the fields, and then clicking the **Add to table** link. This process can be repeated as many times as you want to add entries to the table.

Some predefined types (and their associated data entry forms) include predefined detail tables. You can also create your own custom tables and add them to types. A table is specific to the type to which it was added (i.e., it can't be shared with other types).

To add a detail table to a type

1. From any details summary page, click **Add table**.
2. In the **Details for** field, enter a unique name for the table.
3. Click **Add detail** to define an individual detail that appears as a column in the table. A table must include at least one detail (data field on the form).
4. You can also click **Choose template** to select from a list of existing detail templates that will add several details at once to the table. Each detail appears as a single column in the table.

Details in a table display in the order in which they were entered and can't be moved.

5. When you're done configuring the table, click **Save Details** to save the table. The new table appears in the details list as a Table type. Details display in the list in alphabetical order unless they belong to a specific section.
6. If you want to place the detail table in a specific section on the form, click **Manage sections**, select the section in which you want the table to appear, click **Edit**, and move the table to the **Current Details** box. For more information, see Organizing details in sections.
7. **Important:** Click **Save Details** again (this time from the details summary page) in order to save the changes you've made.

Once a table is configured, you can:

- Edit a table's details by clicking the pencil icon.
- Delete an existing table by clicking the X icon.

Managing detail templates

Use the Detail Templates page to view, create, edit, and delete detail templates. Detail templates are sets or groups of details that make it easy and convenient to add several details at once to a type.

Note: You add a detail template to a type from the type's details summary page, not from the Detail Template page. You can also add a detail template to a table from the table's details summary page.

Asset Manager includes a few predefined detail templates, and lets you create as many new detail templates as you want in order to facilitate the creation of custom types and detail tables.

To create a detail template

1. From the Asset Management menu in the Web console, click **Detail templates**.
2. Click **Add template**.
3. Enter a unique name for the template in the **Details for** field.
4. Add as many details as you want to the template by clicking **Add detail**.
5. When you're done adding details to the template, click **Save Details** to save the template and return to the templates list.

Note: When you add a details template to a type, all of the details contained in that template are added as individual details, not grouped as a template. In other words, a details summary list does not indicate in any way whether details came from a template.

To edit a detail template, click the pencil icon next to the template name.

To delete a detail template, click the X icon next to the template name.

To rename a detail template, click the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)

Adding detail templates

Detail templates are sets or groups of details you can use to add several details at once. You can add detail templates to a type's details summary list or to a detail table.

Detail templates are not specific to a type or table; you can view and add currently available templates from any details summary page.

To add a detail template

1. From any details summary page (for either a type or a table), click **Choose template**. All of the existing detail templates appear in a list, and show all of the details in each template.
2. Find the template you want to add to the details summary, and click **Add template**.

All of the details contained in the template you just added appear as individual details in the details summary. They're not grouped or identified as coming from a template.

3. If you want to place any of the newly added details in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see Organizing details in sections.
4. **Important:** You must also click **Save Details** on the Detail for... page to save any details you've configured.

Using an item list

The item list page provides a summary view of all the items recorded in the database for the type named at the top of the page. To see a type's item list page, click the name of the type on the Assets, Contracts, Invoices, Projects, or Global Lists pages.

The information that displays in the columned table on an item list page is determined by the details that have the Summary option checked. In other words, if Summary is checked then the detail appears on the item list page. You can click the column headings to sort by that detail (data field).

To add items to the database, click the **Add** link, and then fill in the data entry form. For more information, see Adding items.

To edit an item's recorded data, click its **pencil icon**, and then enter new data. When editing, the item's data entry form includes a few extra options. For more information, see Editing an item.

To delete an item from the list (and from the database), click its **pencil icon**, and then click **Delete**.

Additional item list tasks

From an item list page, you can also perform the following tasks:

- Associate items with other items and related information.
- Import data for items of the selected type.
- Export data for items of the selected type.

From the item list page for two asset types, computer and software, you can also:

- Update designated linked details (data fields) with scanned inventory and SLM information from the core database. For more information, see Working with computer assets and Working with software assets.

Adding items to the database

This page is the data entry form for the type named at the top of the page. Asset Manager includes several predefined asset, contract, invoice, project, and global list types, and provides the ability for you to create as many custom types in each of those categories as you like.

When you enter and save the information on a data entry form, the item is recorded in the database.

A slightly different version of this page appears when you're editing an item. For more information, see [Editing an item](#) below.

The contents and layout of a data entry form are defined by the type's details and sections. For more information, see [Using the details summary](#) and [Organizing details in sections](#).

Adding assets—and other important information such as contracts, users, and projects—to the database is *the* central task of someone who wants to gain all the benefits of proactive asset management for their organization. Asset Manager provides the tools necessary to configure asset types and the detail elements that define them, to track that data, and ultimately to analyze and share that data through custom asset reports. However, the benefits of asset management to your business, in real terms, depends on the recorded data itself. If most of the fields in a well-designed and thorough data entry form are left blank, there is very little to track, and running reports will be of minimal value. The recorded data is the key, and hence, data entry should be considered the most important step in implementing an effective asset management solution.

Although the information asked for on data entry forms can vary, the process of adding data is the same, as described below:

To add an item to the database

1. From any item list (accessed by clicking the name of a type on either the Assets, Contracts, Invoices, or Projects page), click **Add**. Or, you can access the same page by clicking the plus sign (+) **Add** link next to the item type.

Note: You can expand or collapse the sections of a form by clicking the section name. Also, refer to the Legend at the top of the form to understand the icons next to certain data fields. Detail icons are explained in [Understanding the detail icons](#).

2. Fill in the data fields. When adding or editing a detail, you can only enter data compatible with the field type (i.e., only an integer in an integer field, a text string in a string field, a date in a date field, etc.).
3. To save the item and continue adding more items, click **Save and add another**.
4. To save the item and return to the item list, click **Save and return to list**.

The new item appears in the item list.

Editing an item

If you're editing an item that has already been added to the database, this page displays the following additional options:

- **Associate items:** Opens the Associate items page where you can create associations between the selected item and other items recorded in the database.

- **Delete:** Removes the item from the item list and from the database. When you delete an item, any association to or from the item is also removed. This data can't be retrieved unless you've exported it beforehand to a CSV file.
- **Print preview:** Opens a print-friendly version of this page in a separate window that can be printed from the browser.
- **Last edited by:** Lets you view (at the bottom of the page) the user who most recently modified this item, their core server, and the time.

Associating items

This page allows you to view, create, and delete associations between the item named on this page and any other item recorded in the database.

Through associations, you can establish and track relationships between any of your fixed assets and their supporting items such as contracts, locations, users, projects, and so on. For example, you may want to associate printers with their lease agreement contract; or PDAs with their users; or phones with their users, locations, and service contracts; and so forth. Associations provide another level of asset management.

Creating associations:

You can create associations only from an actual item page, not from the item list page.

Associations exist between actual items in the database, not between item types. Associations are bidirectional. In other words, if you create an association from a printer to a contract, the same association also exists from the contract to the printer in that specific contract's page.

You can associate the following item types with each other:

- Assets
- Contracts
- Invoices
- Projects

To create an association

1. From any item page, click **Associate Items**. (This is also the way to view an item's associations.)

Note: The Associated Items page refers to the selected item by its key detail.

2. Use the **Search** tool to locate items that you want to associate with the selected item. From the search results list, check the items you want to associate, and then click **Add to list**.
3. Click **Save** to save the associations and return to the item page.
4. Click **Cancel** to exit without saving.

To delete an association, click the X icon next to the association in the list. Deleting an item also removes all of its associations from the database.

Associated item information can be included in Asset Manager reports.

Importing items

Asset Manager provides the ability to import items for asset, contract, invoice, project and global list types. For example, if you have information for all your printers in a single spreadsheet, you could import printer data into the item list for the printer asset type. Importing and exporting lets you use asset management-specific data with other data tracking, database, and reporting tools.

Because you're importing items of a particular type, the **Import** link is only available on a type's item list page.

Required rights

In order to import and export items, a user must have either the Asset Configuration right or the Asset Data Entry right.

Supported file formats

Asset Manager's import and export feature supports both CSV (comma-separated value) as well as XML formatted files. You import data from a CSV or an XML file into an existing type. These file formats are compatible with other data management tools such as Microsoft SQL Server, Oracle, Microsoft Access, and Microsoft Excel.

Understanding the structure of the import file

The file you want to import must be organized in such a way as to accommodate all the details (data fields) used to define the type.

Each line in the import file represents a single item and therefore corresponds to an item row on the item list page. Furthermore, each line must contain the data for that individual item, separated by commas. Each comma-separated value corresponds to a column on the item list page. A line must include a value for every detail in the type. For example, if the type is defined by ten details, then each line in the import file must have ten values (a value can be empty as long as it's separated by commas). Furthermore, the data in each value must match the data type specified for that data field (i.e., integer, string, date, etc.), or the import fails.

It is a requirement that the first line of the import file contain the names of the details (that match the column headings on an item list page), separated by commas.

It might be helpful to envision the import file as basically being in the same format and layout as an item list page—a table listing where each column represents a detail and each line represents an individual item.

Importing items

To import items into an existing type

1. From the Assets, Contracts, Invoices, Projects, or Global Lists page, click the name of the item type you want to import items into.
2. On the item list page, click **Import**.
3. Enter the full path, including the filename, to the file you want to import in the **File path** field. You can click **Browse** to locate and select the file you want to import.
4. Click the **Valid column names** link to see a list of all the details used to define the selected type. A details summary window opens showing all of the type's details by name and other characteristics in a column list.

Important: Your import file's structure and contents must be compatible with the columns in this list (each column representing a detail). For more information on the correct structure of an import file, see Understanding the structure of the import file above.

5. To ignore duplicate data, click **Ignore**. Or, to update duplicate data, click **Update**.

Duplicate data is identified as such by the value of an item's key detail. If two items have the same value for their key detail, both items in their entirety (i.e., their key detail and any other details) are considered duplicate data. You can choose what the import procedure does with any occurrences of duplicate data like this with the **Duplicate handling** feature, as described below:

If you click **Ignore**, any item in the import file whose key detail value is the same as the key detail value of an item that already exists in the database is NOT imported. The item in the import file is ignored and the existing item is preserved.

If you click **Update**, any item in the import file whose key detail value is the same as the key detail value of an item that already exists in the database IS imported. The item in the import file replaces the existing one.

6. Click **Import now**.

If the import file is formatted correctly, the data is added to the database and the items appear on the item list page.

Exporting items

Asset Manager provides the ability to export data for asset, contract, invoice, project, and global list types. Importing and exporting lets you use asset management-specific data with other data tracking, database, and reporting tools.

Because you're exporting items of a particular type, the **Export** link is only available on a type's item list page.

Required rights

In order to import and export items, a user must have either the Asset Configuration right or the Asset Data Entry right.

When you export a type, all of the items currently recorded in the database for that specific type are exported. However, you can customize the data to be included in the export file by selecting which of the type's details you want exported. The selected details will be exported for all the items currently recorded in the database. You can also save a customized list of selected details as an export configuration for future use. Export configurations are specific to the type for which they are created.

Supported file formats

Data can be exported as either a CSV (comma-separated value) formatted file or as an XML formatted file. These file formats are compatible with other data management tools such as Microsoft SQL Server, Oracle, Microsoft Access, and Microsoft Excel.

Understanding the structure of the export file

As stated in the Importing items section, the structure or layout of this exported file essentially matches the layout of an item list page, where each line in the file represents a distinct item record, and each comma-separated value in a line represents a detail (data field) for that item.

Export file names

All items for the selected type are exported in a single file (typename.csv). If the type has table data fields, then each table is exported as a separate file (typename-tablename.csv).

Exporting items

To export items

1. From the Assets, Contracts, Invoices, Projects, or Global Lists page, click the name of the item type you want to export.
2. On the item list page, click **Export**.
3. To use an existing export configuration, select it from the **Configurations** drop-down list.

Or, to manually specify the data you want included in the export file, clear the details you don't want exported. All details are checked by default.

If you want to save your selected details as a new export configuration for this type, enter a name in the **Configurations Name** field, and then click **Save**. The export configuration is added to the drop-down list and can be used at any time by this specific type.

4. Click **Export now**. The Export window opens displaying the files (and formats) that can be exported. You can export one or both of a file's two formats: CSV and XML.

Note on exporting table details

If you're exporting one or more table details for the type, each table detail must be exported as a separate file represented in the Export window by a unique file whose name corresponds to the table name.

5. Click the file you want to export.
6. At the browser's File Download dialog, click **Save**, choose a destination on the local machine, and then click **Save** again.
7. At the Download Complete dialog, click **Close**.
8. You can continue saving other export files from the Export window, and simply click **Close Window** when you're finished.

Using Asset Manager reports

Asset Manager includes a reporting tool that lets you collect and analyze the asset management data you've entered into the database.

The reporting tool includes several predefined asset management-specific reports that you can use to analyze the data you've entered for assets, contracts, invoices, and projects. These predefined reports provide examples of how you create and configure your own custom reports.

To view and edit a report's configuration, click the pencil icon.

To run a report and view the results, click the report name.

To delete a report, click the X icon.

Rights required to use asset reports

A user must have either the Asset Configuration right (which is equivalent to an administrator role for Asset Manager features and implies all Asset Manager rights) or the Reports right to be able to see and use the Reports link and features in Asset Manager. If a user has only the Asset Data Entry right, they won't even see the Reports link in the left navigation pane of the Web console. On the other hand, if a user has only the Reports right, they will see the Assets, Contracts, Invoices, Projects, and Global Lists links, but they can only browse those pages and can't create, edit, or delete any types, details, or actual items. For more information about the specific abilities provided by these asset management rights, see "Using role-based administration with Asset Manager."

Note: A user with only the Reports right does not count against your total number of user licenses for Asset Manager.

Rights are assigned to users by a LANDesk Administrator via the Users tool in the main console.

The Reports right for Asset Manager is the same Reports right that is used to provide access to the reporting tool in the console. Note that none of the Asset Manager reports are available in the main console's Reports tool (even for users with the Reports right). Asset Manager reports are only accessible via the Web console.

Using predefined Asset Manager reports

Asset Manager includes several predefined reports that generate information about the assets, contracts, invoices, projects, and related information recorded in the database. Some of the predefined asset reports are listed below. You can use these reports as examples or templates of what you can do with the Reports tool in Asset Manager.

- Ad-Hoc Projects Completed in Last 30 Days
- Ad-hoc Projects Started in Last 30 Days
- All Computers and Associated Items
- All Consulting Agreements
- All Leases and Associated Items
- All Mobile Phones
- All PDAs
- All Purchase Orders and Associated Items
- Computers by Cost Center Location
- Computers by Requested Date

- Computers Installed in Last 30 Days
- Leases by Business Code
- Leases by Cost Center Location
- Leases Expired in Last 30 Days
- Leases Expiring in Next 30 Days
- Purchase Orders by Cost Center Location
- Purchase Orders by Vendor
- Software by Cost Center Location
- Software by Request Date
- Software Installed in Last 30 Days

Creating and running custom reports

You can create, edit, run, and print your own custom reports.

There are three types of custom reports:

Date report: Provides information for a specific type's recorded items, grouped by one of its date details. For example, you could create a custom date report that gathers information about an asset based on its purchase date, or a contract based on its signature date. The results of a date report are determined by a specified timeframe (range of days) for the date detail. You can customize the additional details that are included in the report.

Summary report: Provides information for a specific type's recorded items, grouped by any one of its details. Summary reports always show a count number and at least one of the item's details. You can customize the additional details that are included in the report.

List report: Provides information for a specific type's recorded items, in a flat list. You can customize the additional details that are included in the report.

Use the procedure below to create and run a custom report:

To create and run a custom report

1. From the Reports page, click the **Add report** link for the type of report you want—date, summary, or list.
2. In the **Report name** field, enter a unique name for the report.
3. From the **Run report on** drop-down list, select whether to report on an asset, contract, invoice, or project type.
4. From the **Select type** drop-down list, select the specific type for whose recorded items you want to gather information. This list includes all the currently available types for the selected category.

If you're creating a **list report**, skip to step 7.

5. For a **date report**:

First, from the **Group by detail** drop-down list, select the date detail you want to base this report on, and under which the items in this report will be grouped. Or, select a global list type (in parentheses), and then select the date detail from its submenu. (The drop-down list includes the currently available *date* details for the selected type, plus any global list types whose date details the selected type uses.)

Then, in the **Timeframe** field, enter the number of days (before or after today) whose dates you want to include in this report. For example, 0 (zero) indicates today, -30 indicates 30 days before today (including today), and 30 or +30 indicates 30 days after today (including today). The date report will include all of the type's recorded items whose specified date value matches a date within this timeframe.

6. For a **summary report**:

First, from the **Group by detail** drop-down list, select the detail you want to base this report on, and under which the items in this report will be grouped. Or, select a global list type (in parentheses), and then select the detail from its submenu. (The drop-down list includes *all* the currently available details for the selected type, plus any global list types whose details the selected type uses.)

Then, if you want the summary report to include only the detail selected above and an item count, clear the **Details** check box. If you clear this option, the Shows columns and Related details options are dimmed and can't be selected. However, if you want to configure additional information to appear in the summary report, make sure **Details** is checked (the default setting), which allows you to select the other information options.

7. Specify the columns (that display details on an item's page) you want to include for each item in the report with the **Show columns** option. You can choose to include just the key detail, the summary details, or all details.
8. Specify additional information you want to include for each item in the report with the **Related details** option. You can choose to include none, table details, or associated items.
9. Click **Save and run** to save this report configuration and generate the report's results. A separate browser (pop-up) window opens and displays the report, which you can view and print.
10. Or, click **Save** to save the report configuration and return to the Reports page without running the report.

If you selected either of the two save options, the report is added to the alphabetical list on the Reports page.

As with predefined reports, you can view and edit a custom report configuration by clicking the pencil icon, and run a custom report by clicking the report name.

You can print a report from the report's pop-up window, according to the browser's Print settings.

Core database installation and maintenance

Using rollup databases

The database Rollup Utility (DBROLLUP.EXE) enables you to take multiple source core databases and combine them into a single destination core rollup database, allowing you to create reports or query the managed devices across your organization. . A core server database can support several thousand devices, and the rollup core device limit depends on your hardware and acceptable performance levels. The source database can be either a core server or a rollup core server.

The system requirements for a destination database may be substantially greater than the system requirements for a standard database. These requirements can vary considerably depending on your network environment. If you need more information about hardware and software requirements for your destination database, contact your LANDesk Software support representative.

Setup installs the database Rollup Utility automatically with the rollup core. The Rollup Utility uses a pull mechanism to access data from cores you select. For database rollups to work, you must already have a drive mapped to each core you want the Rollup Utility to get data from. The account you connect with must have rights to read the core server's registry.

The Rollup Utility checks with a registry key on the core server for database and connection information (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) and uses that key's information to access the database associated with each core you add to the Rollup Utility. For Oracle databases, the TNS definition on the server you're running the Rollup Utility from must match the TNS definition on the core server the utility is accessing.

You can use the rollup utility to select the attributes you want rolled up from the cores. The attribute selections you make apply to all cores. Limiting the number of attributes shortens the rollup time and reduces the amount of data transferred during rollups. If you know you won't be querying on certain attributes, you can remove them.

The Rollup Utility always rolls up the selected attribute data and Software License Monitoring data. You can't customize the Software License Monitoring rollup. Rollup also doesn't include any queries or scopes you've defined. Any console users with rights to the rollup database have access to all data within that database.

Once you've added the core servers you want to roll up and the attribute list for those servers, you can click Schedule to create a scheduled rollup script for each core server. From the rollup core's Web console, you can then schedule these rollup scripts to run at the time and interval you want. Rollup scripts on the rollup core.

To launch the Rollup Utility

1. On a rollup core, run the Rollup Utility (\Program Files\LANDesk\ManagementSuite\dbrollup.exe).
2. Select an existing rollup core server to manage from the list, or click **New** to enter the name of a new rollup core server. Note that you must enter the core server name, and not the database name.
3. Once you select a rollup core, the Source cores list shows cores you've configured to roll up to the selected rollup core.

To configure the attributes that you want to roll up

1. From the Rollup Utility, select the rollup core you want to configure.
2. Click **Attributes**.
3. By default, most database attributes are rolled up. Move attributes that you don't want to roll up from the **Selected Attributes** column back to the **Available Attributes** column.
4. Click **OK** when you're done. Moving attributes to the **Available Attributes** column deletes associated data from the rollup database.

To configure the source core servers for a rollup core

1. From the Rollup Utility, select the rollup core you want to configure.
2. Once you select a rollup core, the Source cores list shows cores you've configured to roll up to the selected rollup core. Click **Add** to add more cores or select a core and click **Delete** to remove one.

WARNING: Clicking delete immediately removes the selected core and all of that core's data from the rollup core database. Also, if you supply an invalid link name when adding a core server to the rollup database, you will have to remove the core from the rollup and re-add it in order to modify the link name.

To schedule database rollup jobs from the Web console

1. From the Rollup Utility, select the **Rollup core** you want to configure.
2. In the **Source cores** list, select the cores you want to schedule for rollup and click **Schedule**. If you don't select any cores, by default all cores in the list will be scheduled when you click **Schedule**. Clicking **Schedule** adds a rollup script for the selected core to the selected rollup core. If you select multiple cores, they will be scheduled as one job and will be processed one at a time.
3. You won't be able to log into a rollup core server from the Web console until at least one core has been rolled up to it. Make sure you use the Rollup Utility's **Rollup** button to manually roll up at least one core.
4. From a Web console, connect to the rollup core server (`<core name>/ldsm/`).
5. In the left navigation pane, click **Scheduled tasks**.
6. Click the rollup script you want to schedule. The script names begin with the source core name followed by the destination rollup core name in parentheses (such as *sample name*).
7. Click **Edit**.
8. Select when you want the roll up to happen and whether it should automatically reschedule or not. When scheduling recurring rollup tasks, make sure there isn't more than one core being rolled up at the same time.
9. Click **Save**.

You can view the rollup task status in the **Status** column. The column displays **All Completed** when the task is finished.)You can also view the status of the task in the Windows Event Viewer.)

Only one rollup can be processed at a time. A scheduled rollup will fail if another rollup is already in progress. When scheduling rollups, allow enough time between rollups that there won't be any overlap. If the rollup times are hard to predict, it's best to schedule all the rollups in a single task. Do this by targeting multiple cores before scheduling. This way, the rollups are handled one at a time automatically.

Increasing the rollup database timeout

With large rollup databases, the Web console's query editor may time out when it tries to query and display a large list, such as the Software Package Name list. When this happens, the list you are trying to display won't show any data. If you experience timeouts you need to increase the database timeout value on the core running the IIS service or the Web console server. At the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core
```

Add a new DWORD, Timeout, with a decimal value of 1800. This value is in seconds. You can adjust this value based on your query types and database performance. Stop and restart the IIS service for the change to take effect.

About the Rollup Utility

Use the database Rollup Utility (run from the rollup core) to manage data rollups from core servers. A rollup core hosts the consolidated data from multiple LANDesk core databases.

- **Rollup core:** You can manage multiple rollup cores from the Rollup Utility. Select the core(s) you want to manage. You first must have a drive mapped to each rollup core.
- **New:** Click to add a new rollup core that you want to manage from the utility. You first must have a drive mapped to the rollup core you're adding. Enter the rollup core's computer name and click **OK**.
- **Attributes:** Click to select the attributes you want rolled up. The attributes list is global for all core servers the selected rollup core uses. Move individual attributes or attribute trees from the **Selected Attributes** column (these attributes will be rolled up) to the **Available Attributes** column (these attributes won't be rolled up).
- **Reset database:** Click to reset the selected rollup database. This deletes all data and rebuilds all tables.
- **Add:** Click to add a core that you want to include data from in the selected rollup core.
- **Delete:** Click to remove the selected core and its data from the selected rollup core's database. **WARNING:** This option deletes the selected core's data from the rollup core when you click **OK**. Data from other core servers remains in the rollup database.
- **Schedule:** Click to add a rollup script for the selected core. If you don't have a core selected in the Source Cores box, this option creates rollup scripts for all cores in the Source Cores box.
- **Rollup:** Click to do an immediate rollup from the selected core. You must have a core selected for this option to be available.
- **Close:** Click to close the Rollup Utility.

Configuring rollup database links

This section describes how to configure database links in all four LANDesk software rollup scenarios. The four scenarios are:

- Oracle rolling to Oracle
- SQL Server rolling to SQL Server
- SQL Server rolling to Oracle
- Oracle rolling to SQL Server

The person doing this configuration must also have access to all DBMSs used by LANDesk, and they must have security permissions to create database links and perform configuration steps at a DBMS server level.

Oracle rolling to Oracle

Configuring the Oracle database

The TNSNames.ora file on the database server in which your rollup database exists must contain an entry for your core server database.

1. For an Oracle 9i* database, within the Enterprise Manager Console, log in to your database. Expand **Distributed**. For an Oracle 8i* database, within the Enterprise Manager Console, log in to your database. Expand **Schema** and your rollup Schema.
2. From the **Database Links** item's shortcut menu, click **Create**.
3. In the **Name** field, enter a name for your database link. **Note:** In the name, LDMS_LINK is the name of the link. If the AR database is using Oracle8i, the link name must match the TNS name of the remote server. If the AR database is using Oracle 9i, the link name can be any name that is not already in use or is reserved. The installation will prompt you for this information.
4. Choose **Fixed User** and enter the username and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (i.e....Net Alias) entry that refers to your core server database.
6. Click **Create**.
7. Double-click your newly-created link and click the **Test** button. You should get a message that says your link is active. You can also test your link by logging into the rollup database and typing the following command:

```
Select count(*) from computer@linkname;
```

If it comes back with the correct number of computers scanned into your core server, your link is set up correctly.

SQL Server rolling to SQL Server

Configuring the SQL Server* database

1. Open SQL Server Enterprise Manager.
2. Expand your server and click **Security**.
3. From the **Linked Servers** item's shortcut menu, click **New Linked Server**.

4. On the **General** tab, do steps 5-11:
5. **Linked Server**: enter a unique name for this database link (for example, LDMS core server1 Link).
6. Choose **Other** data source.
7. Select **Microsoft OLE DB Provider for Microsoft SQL Server**.
8. **Product name**: leave blank.
9. **Data source**: enter the name the database server containing the core database.
10. **Provider string**: enter your provider string. For instance:

```
SQL Server provider=SQLOLEDB.1;user id=<username for the core
server's database>
```

11. **Catalog**: enter the physical name of your core server's database (for example, lddb).
12. On the **Security** tab, do steps 13-14:
13. Select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
14. Open SQL Query Analyzer and type the following command:

```
Select count(*) from [Link name].[database name].[table-owner
name].Computer
```

Using the values above, this query would appear as:

```
Select count(*) from [LDMS Core Server1
Link].[lddb].[dbo].Computer
```

If the correct count comes back, your link is set up correctly.

SQL Server rolling to Oracle

Configuring SQL Server to rollup to Oracle

In order to roll SQL Server to Oracle, you must capitalize all column names in the production SQL database. If you want a utility to do this for you, call LANDesk customer support.

Install Heterogeneous Services for Oracle

1. Using the Oracle Universal Installer, Install the **Oracle Transparent Gateways** for SQL.
2. Edit <oracle home>\rdbms\admin\caths.sql on the Oracle DBMS server so that the two lines that call PRVTHS.PLB and DBMSHS.SQL point to the appropriate directory on Oracle DBMS server.
3. Execute CATHS.SQL using SQL Plus by logging in to SQL Plus and at the prompt typing:

```
@@$ORACLE_HOME/RDBMS/ADMIN/CATHS.SQL.
```

The following error may appear at the end script execution.

```
068: existing state of packages has been discarded
063: package body "LDPROD.DBMS_HS_UTL" has errors
508: PL/SQL: could not find program unit being called
512: at "LDPROD.DBMS_HS", line 629
403: no data found
512: at line 6
```

This error can be caused by an outdated version of JDBC drivers that exists on the Oracle DBMS server. Please call Oracle for troubleshooting and further investigation of your installation if you receive errors during the execution of CATHS.SQL or the scripts that it may call.

Create a UDL file on the core server pointing to the SQL DBMS

1. Create a .UDL file on the core server by right-clicking on the desktop and clicking **New | Text Document**. Save it as <core server name>.udl. Double-click the .udl file and the **Data Link Properties** dialog displays.
2. On the **Data Link Properties** dialog's **Provider** tab, click **Microsoft OLE DB Provider for SQL Server**.
3. On the **Data Link Properties** dialog's **Connection** tab, fill in the database information for the core server's SQL Server database. Click **Allow Saving Password** to save the password information to the UDL file.
4. Click **OK** on the **Data Link Properties** dialog to save the connection information. When prompted whether or not to save the password, click **Yes**.

Create a SID on the Oracle server pointing to SQL Server

1. Copy the ORACLE_HOME/hs/admin/inihsoledb.ora and rename it to init<core server Name>.ora. Copy the UDL file created on the core to ORACLE_HOME/hs/admin.
2. Edit the init<Core Server Name>.ora file. Change the HS_FDS_CONNECT_INFO= line to reflect the path to your UDL file on the Oracle DBMS server. Leave the %_TRACE_LEVEL = 0 parameter equal to 0.
3. Save the init file and close it.
4. Create a listener pointing to the SQL Server by editing the Listener.ora and TNSNAMES.ORA files under ORACLE_HOME/Network/Admin on the Oracle DBMS server.

Sample Entry for TNSNAMES.ORA:

```
<Core Server Name> =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP) (HOST = <Oracle DBMS server>
Name) (PORT = 1521))
  )
  (CONNECT_DATA =
    (SID = <Name of core server>)
  )
  (HS = OK)
)
```

Sample Entry for LISTENER.ORA

```
(SID_DESC =
  (GLOBAL_DBNAME = <Name of core server>)
  (PROGRAM = hsolesql)
  (SID_NAME = <Name of core server>)
  (Oracle_HOME = E:\oracle\ora92)
)
```

5. Restart the Listener Service on the Oracle DBMS server so that the Oracle server will now be able to connect to the SQL Server using OLEDB and Transparent Service.

Create a Database Link using the core server-named SID.

Use the Core Server Name entry in TNSNames.ora file for the Heterogeneous Services link in order to create your link to your SQL Server production database.

1. For an Oracle 9i database, within the Enterprise Manager Console, log in to your database. Expand **Distributed**. For an Oracle 8i database, within the Enterprise Manager Console, log in to your database. Expand **Schema** and your rollup Schema.
2. From the **Database Links** item's shortcut menu, click **Create**.
3. In the **Name** field, enter a name for your database link.
4. Choose **Fixed User** and enter the username and password for the core server's database.
5. In the **Service Name** field, enter the TNSNames.ora (i.e....Net Alias) entry that refers to your core server database.
6. Click **Create**.
7. Double-click your newly-created link and click the **Test** button. You should get a message that says your link is active. You can also test your link by logging into the rollup database and issuing the following command:

```
Select count(*) from computer@linkname;
```

If it comes back with the correct number of computers scanned into your core server, your link is set up correctly.

8. You can also create your link by logging into SQL Plus for Oracle and typing the following SQL statement:

```
create database link "<core server Name(this will be the  
linkname)>" connect to "<sql user name>" identified by  
"<password>" using '<core server Name(this is the SID name)>';
```

Oracle rolling to SQL Server

Configuring Oracle to rollup to SQL Server

Because of a known issue in the Oracle 9i client, it is impossible to use DBROLLUP.EXE to roll an Oracle production database to an SQL Server rollup database using the Oracle 9i client.

It is possible to use the Oracle 10G client to roll an Oracle 9i database to SQL Server. Currently, the Oracle 10G client is not supported in conjunction with LANDesk Management Suite. It can be used though in conjunction with DBROLLUP.EXE in order to allow rollup of an Oracle database to SQL Server based upon the following limitations:

- The Oracle 10G client can't be installed on any server that houses a LANDesk core server, LANDesk additional console, or LANDesk web console server.
- The Oracle 10G client can only be used to point to an existing supported LANDesk production Oracle 9i database.

Create a link to the Oracle database in SQL Server

1. Install the Oracle 10G on the rollup server.
2. Create an Oracle Net Alias to the production Oracle database. The Alias name must be the same as the Alias name used on the core server that uses that database.
3. Open SQL Server Enterprise Manager.
4. Expand your server and click **Security**.

5. From the **Linked Servers** item's shortcut menu, click **New Linked Server**.
6. On the **General** tab, do steps 7-12:
7. **Linked Server**: enter a unique name for this database link (for example, LDMS Core Server1 Link).
8. Choose **Other** data source.
9. Select **Oracle Provider for OLE DB**.
10. **Product name**: leave blank.
11. **Data source**: enter the name the database server containing the core database.
12. **Provider string**: enter your provider string. For instance:


```
provider=ORAOLEDB.ORACLE.1
```
13. On the **Security** tab, do steps 14-15:
14. Select **Be made using this security context** and enter the username and password for the core server's database, then click **OK**.
15. Open SQL Query Analyzer and issue the following command:

```
Select count(*) from [Link name]..[Oracle User Name].COMPUTER
```

Using the values above, this query would appear as:

```
Select count(*) from [LDMS Core Server1 Link]..[Oracle User  
Name].COMPUTER
```

If the correct count comes back, your link is set up correctly.

Multi-core support

The following conditions must be met in order to use multiple cores:

- Both cores must be part of the same domain.
- The domain administrator account must be added the LANDeskManagementSuite local user group on both cores.
- The identity of the LANDesk COM+ application under component services must be set to the domain administrator. This is described in the next section.
- The core.asp file must be edited to include the second core. If this is a dual install, both core files under \inetpub\wwwroot\remote\xml and \inetpub\wwwroot\LANDesk\ldsm\xml must be edited.

To log into a core in a multi-core environment

1. Launch Management Suite on one of the cores.
2. Select the core that you are actually opening Server Manager on from the drop-down menu. Type the user name and password.

Notes

- To successfully complete client configuration, use the correct URL for the core. Otherwise, the configuration will not work.
- You may find it useful to add entries for each core server to your Favorites menu in Internet Explorer. This facilitates switching between cores.

Configuring COM+ server credentials

When using a Web console server that isn't on the core, or if you want to use domain groups inside the LANDesk Management Suite group on the core server, there is some additional server configuration you must do for Management Suite authentication to work correctly. Remote Web console servers must get database connection information and user information from the core server, but since remote Web console servers use impersonated Web credentials on IIS, they can't communicate with the core server directly.

To solve this issue, the Web console server and core server use a COM+ application to communicate via HTTPS, allowing the Web console server to get core server database and user information. You need to configure this COM+ application on the Web console server to use an account that has the necessary rights, such as the domain administrator account. The account that you provide needs to be in the LANDesk Management Suite group on the core server (this allows it to access core server database connection information), and it needs to have rights to enumerate Windows domain members.

If you're using domain groups inside the core server's LANDesk Management Suite group, Management Suite also needs to be able to enumerate Windows domain members. In this case, you also need to provide an account for the core server's LANDesk COM+ application.

To configure the LANDesk COM+ application on a core or remote Web console server

1. Go to the Web server or core server you want to configure.
2. From the Windows Control Panel's Administrative Tools, double-click **Component Services**.

3. Click **Component Services | Computers | My Computer | COM+ Applications**.
4. From the **LANDesk** COM+ application's shortcut menu, click **Properties**.
5. On the **Identity** tab, enter the credentials you want to use.
6. Click **OK**.

Troubleshooting tips

The following troubleshooting tips are for issues that most frequently occur with the console.

I can't activate the core.

If you installed a core, then changed the device time, you will not be able to activate. You must reinstall the product in order to activate the core.

I don't know the URL to the console pages.

Contact the person who installed the core server, most likely the network administrator for your site. However, typically the URL is `http://core server machine name/ldsm`.

Who am I logged in as?

Look above the bar below the name LANDesk Management Suite, at the **Connected As** section.

What machine am I logged in to?

Look above the bar below the name LANDesk Management Suite, at the **Connected To** section.

I launch Management Suite, and I get a "Session Timed Out" message immediately.

If you open Management Suite from the Favorites or Bookmark menu with the "/FRAMESET.ASPX" extension at the end of the URL, Management Suite will not launch correctly. To fix this, edit your Bookmarks or Favorites link to remove this extension, or paste the URL (without the extension) directly into the browser window.

If you don't see some of the left navigation pane links

It's because your network administrator is most likely using LANDesk Server Manager's role-based administration or feature-level security option that limits you to performing certain tasks that you have the rights to do.

The scanner can't connect to the device.

If the scanner can't connect to the device, verify that the Web application directory is configured correctly. If you're using https, you must have a valid certificate. Verify that you have a valid certificate.

I get a permission denied error when I try to access the console

To use feature-level security on Windows 2000 and 2003, you must disable anonymous authentication. Verify the authentication settings on the Web site and the `..\\LANDesk\\ldsm` folder under the Web site.

1. On the server that hosts the Web console, click **Start | Administrative Tools | Internet Information Services (IIS) Manager**.
2. From the **Default Web Site** shortcut menu, click **Properties**.
3. On the **Directory Security** tab, in the **Anonymous access and authentication control** area, click **Edit**. Clear the **Enable anonymous access** option and check **Integrated Windows authentication** option.
4. Click **OK** to exit the dialogs.
5. From the Default Web Site's `..\\LANDesk\\ldsm` subfolder, click **Properties**. Repeat steps 3-4.

I get an invalid session when viewing the console.

It's possible the browser session has timed out. Use your browser's **Refresh** button to start a new session.

The number of items per page is different from the number I specified.

When you specify how many items to display per page, that setting is stored in the Web browser's cookies directory and expires when the console session times out.

The console times out too frequently.

You can change the default session timeout for the console's Web pages. The IIS default is 20 minutes of inactivity before a login expires. To change the IIS session timeout:

1. On the Web server, open the IIS Internet Service Manager.
2. Expand the default Web site.
3. Right-click the **LDSM** folder, then click **Properties**.
4. Under the **Virtual Directory** tab, click **Configuration**.
5. Click the **Application Options** tab, then change the session timeout to the value you want.

Note: LANDesk Management Suite 8.6 is a session-based product. Do not disable the session state.

I cannot view the Remote control page in the Web console.

In order to view the Remote **control** page, you must enable ActiveX controls. Some browsers have ActiveX controls disabled by default. If the Remote **control** page does not load correctly, enable ActiveX controls on your browser by changing the security settings.

I completed the software distribution wizard, but the console did not create a package.

The console uses the IUSR and IWAM accounts on console server. These accounts are originally created based on the computer name. If you have ever changed the computer name, you must follow the steps below in order to successfully create software distribution packages.

1. If you have .Net Framework installed, uninstall it.
2. Uninstall IIS.
3. Reinstall IIS.
4. Reinstall the .Net Framework if you uninstalled it.

A scheduled software distribution job did not run.

If you schedule a software distribution job and it does not start, verify that the Intel Scheduler Service is running on the device.

Also, take into consideration that the scheduling of the job is based on the core server's time. If the job was scheduled on a console that resides in another time zone, the job will start based on the core server's time, which may be different than expected.

Report charts don't display properly.

In order to view the interactive bar and pie charts displayed in many reports, you must have Macromedia Flash Player* 7 installed. Verify that Flash is installed, then run the report again.

Web console error about not being able to authenticate to the database.

If you use an Oracle 9.2.0.1, there is an Oracle install bug that doesn't set the proper permissions for authenticated users (which IIS uses). If you see a Web console error about not being able to authenticate to the database, follow these steps to fix it.

1. Log in to Windows as a user with administrator privileges.
2. Launch Windows Explorer from the **Start** menu and navigate to the ORACLE_HOME folder. This is typically the Ora92 folder under the Oracle folder (i.e. D:\Oracle\Ora92).
3. From the ORACLE_HOME folder's shortcut menu, click **Properties**.
4. Click the **Security** tab.
5. In the **Name** list, click **Authenticated Users**. On Windows XP, the Name list is called **Group or user names**.
6. In the **Permissions** list under the **Allow** column, clear the **Read and Execute** option. On Windows XP, the **Permissions** list is called **Permissions for Authenticated Users**.

7. Re-check the **Read and Execute** option under the **Allow** column (this is the box you just cleared).
8. Click **Advanced**, and in the **Permission Entries** list, make sure you see the **Authenticated Users** listed there with Permission = Read & Execute and Apply To = This folder, subfolders and files. If this isn't the case, edit that line and make sure the **Apply onto** box is set to **This folder, subfolders and files**. This should already be set properly, but it's important that you verify this.
9. Click the **OK** until you close out all of the security properties windows.
10. Reboot your server to make sure that these changes have taken effect.

Oracle error on installation

During installation, you may see the following message:

```
OraOLEDB.Oracle.1 provider is not registered on the local machine.
```

If this happens, it is likely to be a rights issue. You are probably connecting to the Oracle database using a 9i client, and pertains to a known Oracle issue. If you are sure you have already installed the OraOLEDB driver, then try the following:

1. In the Windows Explorer, go to the OraHome92 directory (by default, it is C:\oracle\ora92), right-click this folder and select **Properties**, **Security**, select **Authenticated Users**, uncheck then re-check the **Allow** box for "Read & Execute" permission, then click **Apply**.
2. Click the **Advanced** button, check the **Allow inheritable permissions from parent to propagate to this object** and **Reset permissions on all child objects and enable propagation of inheritable permissions** checkboxes. Click **Apply**, and choose **Yes** when prompted. When this process is over, you'll notice that the **Allow inheritable permissions from parent to propagate to this object** checkbox is checked.
3. In the Command Prompt window, type "iisreset".

At this point, you should be able to authenticate to the database and use your console.

Why am I seeing two instances of the same device in my database?

Have you deleted a device from the core database and reinstalled it using UninstallWinClient.exe?

UninstallWinClient.exe is in the LDMain share, which is the main ManagementSuite program folder. Only administrators have access to this share. This program uninstalls Management Suite or Management Suite agents on any device it runs on. You can move it to any folder you want or add it to a login script. It's a Windows application that runs silently without displaying an interface. You may see two instances of the device in the database you just deleted. One of these instances would contain historical data only, while the other would contain data going forward.

See the *Deployment Guide* for more information on UninstallWinClient.exe.

Using the previous database from LDSM 8.6 or LDMS 8.X on an LDMS/LDSM 8.6 re-installation

If you have uninstalled a previous installation of LDMS 8.X or LDSM 8.6 using the MSDE database on the same machine, the MSDE database and the instance created are not uninstalled, meaning that you can use them again if you want to reinstall LDSM/LDMS 8.6 on the same machine. You can look in the registry for connection information needed to connect to this database during re-install:

Key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\Local
```

the following string values correspond to what need to be filled out in the "User-supplied Database Configuration" page:

```
Server    <hostname\ldmsdata>
User      <sa>
Database  <lddb>
```

Password (this could be encoded, depending on the value of "PWD Encrypted")

When I try to discover an IPMI device, it is not listed in the IPMI folder in the Unmanaged devices page.

IPMI devices must have a BMC (baseboard management controller) that is configured in order to be discovered as IPMI devices and to use full IPMI functionality. If the BMC is not configured, the device can be discovered as a computer. You can then add the device to the list of managed devices and run the Configure Services utility to configure the BMC password. The device's IPMI functionality will then be recognized by this product.

I cannot get the address of the core server when I choose PXE Boot Menu

When trying to run PXE Representative Deployment on a target machine, rebooting the device, pressing F8 and choosing PXE Boot Menu, you get the message "HTGET: Cannot get address for <core server>. Error: Unable to resolve name : <core server> into an address .ParseCoreAddressInof failure

This is because the client is trying to download files from the Core Server using HTTP. The client will use WINS to resolve the Core Server name to IP address. If unable to download the files from the Core Server, HTGET errors will be returned.

To resolve this issue, please read the article

<http://kb.LANDesk.com/al/12/4/article.asp?aid=2558&n=7&tab=search&bt=4&r=0.1898264&s=1>

I added a S.M.A.R.T. drive on a server, but I don't see S.M.A.R.T. drive monitoring in the inventory list for that server.

Hardware monitoring is dependent on the capabilities of the hardware installed on a device, as well as on the correct configuration of the hardware. If a hard drive with S.M.A.R.T. monitoring capabilities is installed on a device but S.M.A.R.T. detection is not enabled in the device's BIOS settings, or if the device's BIOS does not support S.M.A.R.T. drives, monitoring data will not be available, and resulting alerts will not be generated.

Managing local accounts

LANDesk provides an administrative tool that enables you to manage a local machine's users and groups from the console.

Read this chapter to learn about:

- Local accounts overview
- Managing local users
- Managing local groups
- Assigning users to groups
- Changing passwords
- Resetting passwords

Local accounts overview

Local accounts is an administrative tool used to manage the users and groups on local machines on your network. From the console, you can add and delete users and groups, add and remove users from groups, set and change passwords, edit user and group settings, and create tasks to reset passwords for multiple devices. If a device is turned off or not connected to the network, you won't be able to use local account to manage the device.

Note: When using local accounts, the core interacts with the other machines at near real-time.

Using the Core server's local account

Since your core server is a node on your network and has local accounts, you can use the local accounts tool to perform administrative tasks on the server, as well as the console itself. You can add LANDesk users to the console by creating local users and adding them to the Windows NT **LANDesk Management Suite** group. This enables you to perform administrative tasks from the console, without having to use the native local accounts management system, such as Computer Management on Windows NT.

If you prefer, you can still use the native local accounts management system to manage local accounts. You can access the devices directly, remote control the machines from the console, or use a third-party tool to access the devices and perform the administrative tasks.

For more information on using the console to perform local accounts management, see [Managing LANDesk users](#).

Managing local users

You can add, delete, and edit users on a local machine from the console.

To add a user

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Users** and then click **Add**.
4. In the **New User** dialog, enter a user name, a full name, and a description.
5. Enter a password, confirm the password, and specify the password settings.
6. Click **Save**.

To delete a user

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to delete and then click **Delete**.
5. Click **Yes** to verify the procedure.

To edit a user

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.

4. Right-click the user you want to edit and then click **Edit**.
5. Make your desired changes and then click **OK**.

Managing local groups

You can add, delete, and edit groups on a local machine from the console.

To add a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, right-click **Groups** and then click **Add**.
4. In the **New Group** dialog, enter a group name and a description.
5. (Optional) Add users to the group by clicking **Add**.
6. Click **Save**.

To delete a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to delete and then click **Delete**.
5. Click **Yes** to verify the procedure.

To edit a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to edit and then click **Edit**.
5. Make your desired changes and then click **OK**.

Assigning users to groups

There are two methods for adding and removing users to and from groups on a local machine from the console. The first method allows you to add or remove multiple users to or from a group at one time. The second method allows you to add or remove the selected user to or from one or more groups.

To add users to a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to add users to and then click **Edit**.
5. In the **Edit group** dialog, click **Add**.
6. Select the users you want to add to the group and then click **Add>>**.
7. Click **OK**.
8. Click **OK** in the **Edit group** dialog.

To add a user to one or more groups

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to add to one or more groups and then click **Edit**.
5. In the **Edit user** dialog, click the **Member of** tab.
6. Click **Add**.
7. Select the groups you want the user to belong to and then click **Add>>**.
8. Click **OK**.
9. From the **Edit user** dialog, click **OK**.

To remove users from a group

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Groups**.
4. Right-click the group you want to remove users from and then click **Edit**.
5. Select the users you want to remove and then click **Remove>>**.
6. Click **OK**.

To remove a user from one or more groups

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to remove from one or more groups and then click **Edit**.
5. In the **Edit user** dialog, click the **Member of** tab.
6. Select the groups you want the user to be removed from and then click **Remove>>**.
7. Click **OK**.

Changing passwords

You can change a user's password on a local machine from the console.

To change a user's password

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Right-click the user you want to change the password for and then click **Set password**.
5. Enter a new password, confirm the password, and then click **OK**.
6. Click **OK** to verify the password has been changed successfully.

Resetting passwords

You can create a scheduled task to reset the password for a specific user name. Once the task has been scheduled, you are taken to the **Scheduled tasks** tool where you can specify the target devices and the start time. For example, from a local account you could create a task to reset the password for the **Administrator** user name. You would then designate the target devices and schedule when the task will occur. Once the task is run, all administrators wanting to authenticate to the target devices would have to use the new password.

To reset the password

1. In the console, from the **Network View**, click **Devices | All devices**.
2. Right-click the device you want to manage and select **Manage local users and groups**.
3. In the **Local users and groups** dialog, click **Users**.
4. Click the **Schedule** icon.
5. In the **Schedule task** dialog, insert the user name that you want to reset the password for. You can select an existing user name from the drop-down list, or type a different one.
6. Enter a new password, confirm the password, and then click **Schedule**.
7. From the **Scheduled tasks** tool, right-click on the scheduled task and then click **Properties**.
8. From the **Scheduled tasks - properties** dialog, designate the target devices and enter the scheduling information. For more information, see [Scheduling tasks](#).
9. Click **Save**.

Using the file replicator

The LANDesk file replicator is a utility designed to replicate files from a remote Web server to the local system. It provides the following features:

- **File and directory support:** Replicate individual files or directories. Directory support can be recursive.
- **Multiple task support:** Multiple download tasks can be defined and run simultaneously. Each task can download resources located in different Web servers.
- **Bandwidth control:** A maximum bandwidth in percentage or actual transmission rate can be specified that will not be exceeded during the replication operation.
- **Restartable copying:** If a copy operation is interrupted because the connection is lost or time runs out, replication will resume from the point where it was interrupted when the job is relaunched.

Your Web server must be configured properly for the file replicator to work:

- The Web server's "directory browsing" option must be enabled.
- Some application extensions, such as .ASP and .ASPX, have special meanings in the Web server. You must remove the application extension for these kinds of files if you want to replicate them from a Web server.

Using the file replicator

The file replicator copies files from Web sites or Web shares to a folder you specify. You can create periodic repeating tasks or single tasks that run on a schedule you specify. The file replicator uses the same HTTP transfer technology that Management Suite uses for software distributions. You can limit the transfer bandwidth by kilobytes per second or by a percentage of available bandwidth.

Management Suite setup copies the file replicator to the \Program Files\LANDesk\ManagementSuite\Utilities\File Replicator folder. The replicator is a standalone Windows application and you can copy the File Replicator folder and subfolders to any server you want. If you want to access the online help, also copy Idms.chm to the same place.

To configure a replication task, you need to provide the following:

- Task parameters, such as the schedule, target folder, and bandwidth options
- Source URLs. If you specify multiple URLs, they are processed one at a time.

The file replicator caches files in the **Temporary folder** box. Once the copy finishes to the temporary directory, the replicator copies the file to the destination and deletes it from the temporary directory. This prevents partial copies from ending up on the destination if the file copy from the source is interrupted for some reason.

The file replicator stops whatever it's doing when it's opened. When you're done with the window, make sure you click **Start download**. This minimizes the replicator to the system tray and allows replication tasks to execute.

To create a replication task

1. Launch the file replicator.
2. From the **New** button's menu, click **New periodic task** or **New single task**.
3. Enter a task **Name**.
4. Enter or **Browse** for the **Destination folder**.
5. Enter or **Browse** for the **Temporary folder**.
6. Set the time you want the replication task to occur. If the task doesn't finish in the time allowed, it will resume from the point it left off the next time the task runs.
7. Select the bandwidth options you want. You can specify a value in kilobytes per second, a percentage of available bandwidth, or none.
8. Click Add to enter source URLs. The address must be in the form of http://server/path. If necessary, specify the credentials necessary to access the URL. When you're ready, click **Browse**. If the URL and credentials work, you'll see the destination in the lower half of the dialog. Check **Download recursively** if that's what you want. Click OK when you're done.
9. Repeat step 8 for each URL you want to replicate.
10. Click **Save** when you're done.
11. When you're done configuring tasks, click **Start download** to activate file replication on the schedule you specified. The file replicator minimizes to the system tray.

The file replicator stores a log of its actions.

To view the file replicator log

1. Launch the file replicator.
2. Click the **View log** toolbar button.

You can reschedule a single task. This resets the task so it will run again.

To reschedule a task

1. Launch the file replicator.
2. Select the single task you want to reschedule.
3. Click the **Reschedule task** toolbar button.

Understanding the bandwidth options

The file replicator uses bandwidth options to make sure replication doesn't saturate a device's available bandwidth. Any bandwidth options you specify apply to the device the replicator is copying files from, not the destination. There are two bandwidth options the replicator can use:

- **Value(KB):** The amount of bandwidth, in kilobytes/sec, that the job can use. Values must be in the range of 2 to 10000.
- **Percentage(%):** The amount of network bandwidth. Values must be in the range of 5 to 100.

Bandwidth options are set on a per-job basis. If you have multiple file replication jobs active at once, the job bandwidth settings can interact. For example, if you have one job that's allowed 100 KB/sec second, and another that's allowed 50 KB/sec, the total bandwidth used if the two jobs are active at the same time will be 150 KB/sec. With percentage of available bandwidth, it's slightly more complicated. If you have two jobs that are allowed 50% of available bandwidth, the total bandwidth used by both jobs won't exceed 50% of the total. Each job will end up with about 25% of the available bandwidth.

Managing Macintosh devices

LANDesk provides the most complete system management for Apple Macintosh computers and devices. This enables IT professionals to automate systems management tasks throughout the enterprise. From the console, you can gather and analyze detailed hardware and software inventory data from each device. Use the data to select targets for software distributions and to establish policies for automated configuration management. Manage software licenses to save costs and monitor compliance with license agreements. Remote control devices to resolve problems or perform routine maintenance. Automate remote image deployment and migrate device profiles to streamline new device provisioning and existing device migration. Keep track of your inventory and produce informative reports.

Read this chapter to learn more about:

- LANDesk for Macintosh overview
- Tools for Macintosh
- Agent configuration
- Inventory
- Software distribution
- Managed Scripts
- Remote control
- Operating system deployment
- Reports
- Scheduled tasks
- Software license monitoring
- Security and patch manager
- Managing a client Macintosh machine

LANDesk for Macintosh overview

This chapter pertains to how LANDesk is used to manage Macintosh computers. It provides a central location for referencing specific information on Macintosh-related tasks, tools, features, and functionality. For broader information about using tools and features to manage your network, refer to the chapter pertaining to the tool of interest. For more information, see [Console overview](#).

Tools for Macintosh

LANDesk consists of several tools and features you can use to manage the computers and devices on your network running Macintosh operating systems. Only devices running Mac OS X and Mac OS 9 are supported. Not all tools and features used to manage Mac OS X devices are available for managing Mac OS 9 devices.

The following table lists the tools and features available on Mac operating systems:

Tools	Mac OS X features	Mac OS 9 features
Agent configuration	<ul style="list-style-type: none"> • Custom preferences • Update agent configuration 	<ul style="list-style-type: none"> • Custom preferences • Update agent configuration
Inventory	<ul style="list-style-type: none"> • Inventory scans 	<ul style="list-style-type: none"> • Inventory scans
Software distribution	<ul style="list-style-type: none"> • Push-based distribution 	<ul style="list-style-type: none"> • Push-based distribution
Managed scripts	<ul style="list-style-type: none"> • File download • Shell command / AppleScript execution • Targeted Multicast 	<ul style="list-style-type: none"> • File download • AppleScript execution
Remote control	<ul style="list-style-type: none"> • Control/observe • File transfer • Chat • Remote browse and execution • Reboot • Wallpaper suppression • Color-depth reduction • Keyboard and mouse lockout • Screen blanking 	<ul style="list-style-type: none"> • Control/observe • File transfer • Chat • Remote browse and execution • Reboot • Wallpaper suppression • Color-depth reduction
OS deployment and profile migration	<ul style="list-style-type: none"> • Capture image • Deploy image 	<ul style="list-style-type: none"> • Capture image • Deploy image
Reports	<ul style="list-style-type: none"> • Custom reports • Report designer 	<ul style="list-style-type: none"> • Custom reports • Report designer
Schedule Tasks	<ul style="list-style-type: none"> • Task actuation 	<ul style="list-style-type: none"> • Task actuation
Software license	<ul style="list-style-type: none"> • Application monitoring • Application denial 	

monitoring	<ul style="list-style-type: none"> • License compliance tracking and reporting 	
Security and patch manager	<ul style="list-style-type: none"> • Detection <ul style="list-style-type: none"> • Apple security announcements • Apple system updates • Product updates • Remediation <ul style="list-style-type: none"> • Policy • Push • Auto-fix 	

For more information, see Using Management Suite tools.

Agent Configuration for Macintosh devices

LANDesk uses agent configurations to gain control of devices and manage them. Agents are components provided by the server to the client devices that make them fully manageable from the console. Macintosh devices first need to have the default agent configuration loaded. Then additional configurations can be created and applied.

Loading the default Agent Configuration for Macintosh devices

The Default Mac Configuration package contains the required agents for controlling Macintosh devices. In order to gain control of your Macintosh devices, you need to:

1. Obtain the necessary package (agents).
2. Deploy the agents to the devices.
3. Install the agents on the machines.

After the default agents have been installed, your devices become managed devices. Then you can create custom configurations to have greater control of your Macintosh devices. Custom agents are easily implemented once your devices are managed.

Note: All devices must support TCP/IP.

Obtaining the package (agents) for Macintosh devices

You can obtain the default package from the LDLogon/Mac shared folder on your core server. The LDLogon/Mac folder is automatically created during the installation of LANDesk. Since the LDLogon folder is a Web share, it is available from the Internet at <http://<CoreServerName>/LDLogon/Mac>. The packages you need depend on the operating system version:

OS version	Package
Mac OS X	Default_Mac_Configuration.pkg.zip
Mac OS 9	Default_Mac_Configuration.ini LANDesk_Classic_Client.sit

Deploying agents to Macintosh devices

You need to decide on a deployment method to place the agents on the target Macintosh devices. Since there are no domain-level administrative accounts that give you access to Macintosh devices, there are no login scripts for Macintosh devices, and Apple ships with all services disabled for security reasons, the only way to natively deploy the agents is to perform the procedure manually. Due to these difficulties, in many organizations the only way to initially deploy the Mac OS X agents is to:

- Access the agent using a Web browser from LDLogon/Mac (see Obtaining the package (agents) for Macintosh devices).
- E-mail the configuration package to users.
- Put the configuration package on a CD or other removable media and take it to each Macintosh device.

There are third-party Macintosh software distribution applications you can use to deploy the agents to the devices (some install agents simultaneously). Otherwise, you'll have to deploy the agents manually as described above. The third-party software distribution applications for Macintosh are:

- Apple Remote Desktop
- Apple Network Administrator
- netOctopus
- Timbuktu
- FileWave
- FoolProof
- Secure Shell (SSH)

Use your deployment method to place the appropriate package with the corresponding agents on the target devices.

Installing agents on Macintosh devices

Once you have deployed the agents to the target devices, you need to install them on the machines. You must have the LANDesk agents installed on your Macintosh devices before you can manage them. After you've installed the base agents, subsequent agent deployments and updates are easily handled through the existing agents.

To install agents for Mac OS X devices

1. On the client machine, locate **Default_Mac_Configuration.pkg.zip** or access the package from the Web share (see Obtaining the package).
2. Unzip the file or copy the files to the target device.
3. Double-click **LDMSClient.pkg**.
4. Reboot the machine.

To install agents for Mac OS 9 devices

1. On the client machine, locate **LANDesk_Classic_Client.sit** and **Default_Mac_Configuration.ini** or access them from the Web share (see Obtaining the package).
2. Decompress **LANDesk_Classic_Client.sit**, if not already decompressed. This will create the **LANDesk Classic Client** folder.
3. Select the **Default_Mac_Configuration.ini** file and rename it **com.landesk.ldms.ini**.
4. Drag and drop the **com.landesk.ldms.ini** file into the **LANDesk Classic Client** folder and replace the old **com.landesk.ldms.ini** file with the new file you just renamed. If prompted, overwrite the file.
5. Launch the **Mac Client Install**.
6. Reboot the machine.

Creating agent configurations for Macintosh devices

Use the Agent configuration tool to create and update custom configurations for your Macintosh devices, such as what agents are installed on devices and what network protocols the agents use. You can create different configurations for your specific needs, such as a configuration for devices using a particular operating system, or one for the devices located in your accounting department.

In order to push a configuration to devices, you need to create or update an agent configuration and schedule the task to occur.

Creating or updating the agent configuration

Set up specific configurations for your devices.

To create an agent configuration for Macintosh devices

1. Click **Tools | Configuration | Agent configuration**.
2. Click the **New Mac** button to create a new Macintosh configuration.
3. Complete the Agent configuration dialog. For more information, see Using the agent configuration dialog (for Macintosh), or click Help in the dialog.
4. Click **Save**.

To update an agent configuration

1. Click **Tools | Configuration | Agent configuration**.
2. Right-click the agent configuration to be updated and select **Properties**.
3. Make the updates to the agent configuration.
4. Click **Save**.

Scheduling the agent configuration

You can push agent configurations to devices that have the standard LANDesk agent or remote control agent installed. Use the **Scheduled tasks** tool to run your new or updated agent configuration.

To schedule an agent configuration for Macintosh devices

1. Click **Tools | Configuration | Agent configuration**.
2. Right-click the agent configuration to be scheduled and select **Schedule**.
3. Make the updates to the agent configuration.

Manually running agent configuration for Macintosh devices

You can manually run agent configurations for Macintosh devices once they have been created or updated. When an agent configuration is created (**Tools | Configuration | Agent configuration**), the following files are created in the LDLogon/Mac folder on your core server:

- **<agent configuration name>.pkg.zip** (for Mac OS X devices)
- **<agent configuration name>.ini** (for Mac OS 9 devices)

The LDLogon/Mac folder is a Web share and should be accessible from any browser. Follow the instructions for Loading the default Agent Configuration for Macintosh devices. Insert your agent configuration files instead of the default files.

Uninstalling Mac OS X

If you want to uninstall the Mac OS X agents, run the uninstall script, **lduninstall.command**, located on each device in the /Library/Application Support/LANDesk folder. You will need to provide an administrator password.

Uninstalling Mac OS 9

If you want to uninstall the Mac OS 9 agents, run the uninstall script from: **HD:System Folder:Application Support:LANDesk:Mac Client Uninstall**.

Using the Agent configuration dialog (for Macintosh)

This section describes the agent configuration dialog for Macintosh devices. The dialog consists of the following:

- Application policy management
- Apple base agent
- Remote control
- Standard LANDesk agent

About the Application policy management page

Use this page to specify the port the policy-based distribution agent will use to communicate with the core server. The default port is 12175. You'll need to make sure this port is open on any firewalls between devices and the core server. If you change this port, you'll also need to change it on the core server. You can change the port the QIP server service uses by editing the following registry key:

HKLM\Software\Intel\LANDesk\LDWM\QIPsrvr

About the Apple base agent page

Use this page to configure the inventory scanner.

- **Send scan to LDMS core server:** Enter the core server name or IP address. This is the server the agent sends scan information to. No scan information goes to the core database unless this server address is correct.
- **Save scan in directory:** The directory where the data from the scan is saved. If you select both the core server option and this option, the scan information will go to both location.
- **Choose scan components:** Select the components you want to scan. Not selecting all components may slightly increase scanning speed.
- **Force software scan:** Forces the device to do a software scan with each inventory scan, regardless of whether the core server indicates one is due.

- **Scan applications folder only:** For software scans, only scans for applications in the applications folder. This can increase scanning speed, though it will miss applications stored outside this folder.

About the Remote control page

Use this page to configure the remote control agent.

- **Give control to user:** Permits a remote user to control this device in these situations:
 - **Always:** From any domain, whenever necessary.
 - **From same domain:** From the same domain only.
 - **By session:** On a session-by-session basis. Each time an administrator tries to start a remote control session, a dialog pops up letting the user prevent the session or allow it to continue.
- **Open applications and files:** Permits a remote user to open files on this device.
- **Copy items:** Permits a remote user to copy files to and from this device.
- **Delete and rename items:** Permits a remote user to delete or rename files that reside on this device.
- **Lock keyboard and mouse:** Permits a remote user to lock your keyboard and mouse during a remote control session. This option prevents you from interfering with remote actions.
- **Blank screen:** Permits a remote user to make your screen go blank during a remote control session. This option is useful if your device contains sensitive documents that an administrator may need to open remotely without letting others read if they happen to walk by your device monitor.
- **Restart and shut down:** Permits a remote user to restart or shut down your device.
- **Control and observe:** Permits a remote user to remote control and observe your actions on this device. The administrator can't do anything except watch your actions.
- **Show when being observed:** When a remote control session is active, display a visual cue in the menu bar.

About the Standard LANDesk agent page

Use this page to configure agent security and management scope. For more information on agent security, see Agent security and trusted certificates. For more information on scope, see Using role-based administration.

- **Trusted certificates:** Lists the certificates on the core server. The client must have a certificate that matches the certificate on the core server for agent communication to be authorized. These certificates are used to authenticate agent communication. The remote control agent for Macintosh doesn't use a certificate.
- **Path:** Defines the device's computer location inventory attribute. Scopes are used by role-based administration to control user access to devices, and can be based on this custom directory path. The path is optional.

Inventory for Macintosh devices

The inventory scanning utility is used to add Macintosh devices to the core database and to collect device hardware and software data. When you configure a device, the inventory scanner is one of the components of the LANDesk agent that gets installed on the device. The inventory scanner runs automatically when the device is initially configured. A device is considered managed once it sends an inventory scan to the core database.

The scanner executable for Mac OS X devices is named **ldscan** (UNIX is case sensitive). These devices can be configured to scan at boot-up, at log in, at wake from sleep, and at network change. You can also set up a cron job to schedule the inventory scan to occur at a regular interval. The scanner executable for Mac OS 9 devices is named **LANDesk Inventory Agent**. These devices only scan at boot-up.

With the inventory scanner, you can view summary or full inventory data. You can print and export the inventory data. You can also use it to define queries, group devices together, and generate specialized reports. For more information about the Inventory tool, see [Managing inventory](#).

Note: Macintosh devices don't support delta scanning, scan compression, scan encryption, and data forms.

Software Distribution for Macintosh devices

Software distribution enables you to deploy software and file packages to Macintosh devices on your network running Mac OS X. Devices receiving the software distribution packages must have the following LANDesk agents installed:

- LANDesk client agent
- Software distribution agent

You can distribute single-file executable packages to Mac OS X devices. Each distributed package consists of only one file, and the agent will try to install the file once the device receives it. Any file can be downloaded. Install packages (.PKG) can also contain directories, but they must be compressed. If the file downloaded has a suffix of .SIT, .ZIP, .TAR, .GZ, .SEA, or .HGX, LANDesk will decompress the file before returning. (Users should make sure that Stuffit Expander* has its "check for new versions" option disabled; otherwise a dialog may interrupt the software distribution execution.)

Note: You must install LANDesk's Mac OS X agent on the target devices before you can distribute files to them.

You can schedule Mac OS X distributions in the Scheduled tasks window and drag Mac OS X devices into the Scheduled tasks window as distribution targets (see Scheduled tasks for Macintosh devices).

A distribution package consists of the package files you want to send, and distribution details, which describe the package components and behavior. You must create the package before it can be delivered and run. The following instructions explain how to perform software distribution. In order to execute it correctly, the software distribution package must exist on either a network or Web server and the recipient devices must have the software distribution agent installed.

There are three main steps required to distribute a package to devices:

1. Create a distribution package for the software you want to distribute
2. Create a delivery method
3. Schedule the script for distribution

To create a distribution package

1. Create the package you want to distribute.
2. Click **Tools | Distribution | Distribution Packages**.
3. Under **My distribution packages**, **Public distribution packages**, or **All distribution packages**, right-click **Macintosh** and select **New distribution package**.
4. In the **Distribution package** dialog, enter the package information and see the options. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your distribution appears under the tree item for the package type you selected.

To create a delivery method

1. If you've already configured a delivery method that you want to use, skip to the next procedure (To schedule a script for distribution).
2. Click **Tools | Distribution | Delivery Methods**.

3. Right-click the delivery method you want to use and then click **New delivery method**.
4. In the **Delivery method** dialog, enter the delivery information and change the options you want. For more information on each page, click **Help**.
5. Click **OK** when you're done. Your script appears under the tree item for the delivery method you selected.

To schedule a script for distribution

1. Click **Tools | Distribution | Scheduled Tasks**.
2. Click the **Create software distribution task** toolbar button.
3. On the **Schedule task** page, enter the task name and the task schedule.
4. On the **Delivery Methods** page, select the delivery method you want to use.
5. On the **Distribution package** page, select the package script you created.
6. On the **Target machines** page, add the devices you want to receive the package.
7. On the **Summary** page, confirm the task is configured correctly.
8. Click **OK** when you're done.

View the task progress in the Scheduled tasks window.

You can use queries to create a list of devices to deploy a package to. For information on creating queries, see Using database queries.

Macintosh software distribution commands

Macintosh software distribution commands are download commands, as opposed to a shell command (see Managed scripts for Macintosh devices). Download commands begin with either "http://" or "ftp://". If it's not a download command, it's a shell command by definition. The following is an example of a download command:

REMEXEC0=http://...

A download command won't autorun any files. After downloading the file to devices, you can follow up with a shell command to execute the file. Files are downloaded to /Library/Application Support/LANDesk/sdcache/, which you need to be aware of in your shell commands.

Note: If you're hosting files on a Windows 2003 server, you need to create MIME types for the Macintosh file extensions, such as .SIT, otherwise the 2003 server won't let you access the files. The MIME type doesn't have to be valid, it just needs to exist.

Configuring policies for Macintosh devices

You can also create Macintosh device policies (Mac OS X only). Creating a Macintosh device policy is similar to creating a policy for a Windows-based device. Macintosh devices also have the same required, recommended, and optional policy types. Macintosh application packages must be a single-file format. Policy-based management will check for policy updates during login and when waking up from sleep. When targeting policies, Macintosh devices don't support policy-based management by user name, only by device name.

Policy-based management does the following with Macintosh application policy packages:

1. Downloads files to /Library/Applications/LANDesk/sdcache (just like software distribution downloads).
2. If the download is compressed, policy-based management will decompress it in place.

3. If the download is a disk image, policy-based management will mount it, look for the first Apple Package Installer file found on the mounted volume, run it silently, and then unmount it.
4. If the download is an Apple Package Installer file, policy-based management will run it silently.

Also, policy-based management does support .DMG files with EULAs.

Note: Some package types don't work well with software distribution.

Installer Vise and Installer Maker installers don't work well with policy-based management. They almost always require user interaction and can be canceled.

To add a Macintosh client policy

1. Click **Tools | Distribution | Delivery methods**.
2. Configure a Hybrid or Policy delivery method for the package you want to distribute.
3. Click **Tools | Distribution | Scheduled tasks**.
4. Click the **Create software distribution task** button.
5. Configure the task. Click **Help** on each page if you need more information.

To refresh the local client policies

1. In the Management Suite Preference Pane on the Macintosh device, click the **Overview** tab.
2. Click **Check now** for application policy management.

To view installed policies

1. In the Management Suite Preference Pane on the Macintosh device, click the **APM** tab.

Managed scripts for Macintosh devices

LANDesk uses scripts to execute custom tasks on devices. You can create scripts from the **Manage scripts** window (**Tools | Distribution | Manage scripts**). Macintosh scripts use shell commands to execute files. Shell commands run as root. The scripts are saved as text files, and you can edit them manually if you need to once they're created. The following is an example of a shell command:

REMEXEC0=...

The user can use the shell command "open" to launch files and applications, or "installer" to install .PKG files. It's also possible for the download file to be a shell script written in Perl, Ruby, Python, and so on.

When files are downloaded, they are saved to /Library/Application Support/LANDesk/sdcache/, which you need to be aware of in order to execute some of your shell commands.

You can schedule Mac OS X managed scripts in the Scheduled tasks window and drag Mac OS X devices into the Scheduled tasks window as script targets (see Scheduled tasks for Macintosh devices).

Remote control for Macintosh devices

You can remote control a Macintosh device from the console the same way you would a Windows device. Before you can perform any remote control tasks, you must connect to the target device. Only one viewer can communicate with a device at a time, though you can open multiple viewer windows and control different devices at the same time. When you connect to a device, you can see the connection messages and status in the Connection messages pane, if that is visible. If it isn't, you can toggle it by clicking **View | Connection messages**.

Macintosh keyboards have some keys that PC keyboards don't. When remote controlling a Macintosh, the following keys are used on the PC keyboard to emulate a Macintosh keyboard:

- The Alt keys map to the Command key.
- The Window keys map to the Option key.

You need to have system key pass-through enabled in the remote control viewer window for the Alt and Windows keys to pass their Macintosh mappings.

To connect to a device

1. In the **Network view**, right-click the device you want to remote control, and then click **Remote control**, **Chat**, **File transfer**, or **Remote execute**.
2. Once the viewer window appears and connects to the remote device, you can use any of the remote control tools available from the **Tools** menu, such as chat, file transfer, reboot, inventory, or remote control.
3. To end a remote control session, click **File | Stop connection**.

For more information, see Using remote control.

Operating system deployment for Macintosh devices

The operating system deployment (OSD) feature uses the agent-based deployment method to deploy OS images to Macintosh devices. This method uses a device's existing OS and installed LANDesk agents to deploy the images.

For more information, see Using OS deployment.

Note: OSD for Macintosh is only supported by devices running Mac OS X. Profile migration for Macintosh devices is not currently supported.

WARNING: OS deployment (imaging) should be used with caution. Operating system deployment includes wiping all existing data from a device's hard drive and installing a new operating system. There is a substantial risk of losing critical data if the OS deployment is not performed exactly as described in this document, or if poorly implemented images are used. Before performing any OS deployment, we recommend that you back up all data in such a manner that any lost data may be restored.

OSD Prerequisites for Macintosh devices

Before you can run OSD for Macintosh devices, you need a Mac OS X Server (also called your NetBoot or Bootp server) with a NetBoot image created and the LANDesk client installed. LANDesk uses standard .DMG files for creating and deploying images to Macintosh devices. Make sure the NetBoot image is marked as diskless in Sever Admin. Also, make sure the com.landesk.uuid.plist file is removed from the /Library/Preferences folder of your NetBoot image. If you leave the file in your image, all devices using the image will have the same core database entry. OS deployment will install the LANDesk agents after the image is deployed. When OS deployment places an image on a target device, it uses the existing partition on that device. Only single partitioning is supported for Macintosh devices.

For more information on NetBoot usage and setting up your Mac OS X server, see your Macintosh documentation. You will need to provide the IP address of your BootP (NetBoot) server in order to perform OSD for Macintosh devices.

What happens during OS deployment

The following occurs during OSD:

1. LANDesk connects to the target device and runs any preconfiguration commands you specify in the OSD script.
2. The device is configured to boot from the NetBoot server.
3. The device boots from the NetBoot server.
4. The new Mac OS is deployed to the device.
5. The settings are restored to the device.
6. The device boots locally from its own image.
7. The user logs in using their profile.

Note: Using the Collection Manager dialog to create a user-initiated profile migration package is not supported for Macintosh devices.

Creating imaging and profile migration scripts for Macintosh devices

Use the Create an OS deployment script wizard to create image capture and image deploy scripts for Macintosh devices. All scripts are managed with the Manage Scripts tool (**Tools | Distribution | Manage scripts**).

For descriptions of the pages in the wizard's interface, see Macintosh Help.

With the wizard, you can create scripts that perform the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.

Once you have created a script, you can schedule it to run on devices by using the **Scheduled tasks** tool.

To create an OSD script

1. Click **Tools | Distribution | Manage scripts**.
2. In the Manage Scripts window, right-click **All OSD/Profile migration Scripts** and then click **New Macintosh OSD** in the shortcut menu to open the script selection dialog.
3. Select the type of script you want to create and click **OK**.
4. Insert the required information on each page.
5. Click **Finish**. The script appears in the All OSD/Profile Migration Scripts group in the Manage Scripts window. For more information on each page, click **Help**.

To schedule a script for OSD or profile migration

1. Click **Tools | Distribution | Manage scripts**.
2. Expand the **All OSD/Profile migration Scripts** tree.
3. Right-click the desired script and select **Schedule**.
4. From the Schedule tasks window, right-click on the script and select **Properties**.
5. In the dialog, click **Schedule task**.
6. Enter the desired scheduling information and click **Save**.

Reporting for Macintosh devices

The reporting tool enables you to generate a wide variety of specialized reports that provide critical information about the Macintosh devices on your network. The reporting tool operates the same way for all operating systems. For more information, see [Using reports](#).

Scheduled tasks for Macintosh devices

The scheduled tasks tool actuates or starts many of the tasks you set up or configure in the application. These tasks can be run immediately, scheduled to occur at a later time, or configured to run on a regular basis. Both the core server and managed devices have services/agents that support scheduled tasks. For more information, see *Using scripts and tasks*.

Note: Before you can schedule tasks for a device, it must have the standard LANDesk agent installed and be in the inventory database.

The following procedures require the use of the scheduled tasks tool:

- Agent configuration deployment
- Software distribution
- Managed scripts
- Operating system deployment
- Security and patch manager

Software license monitoring for Macintosh devices

Macintosh devices running Mac OS X support software license monitoring. With each inventory scan, the Macintosh software monitoring agent sends information to the core server about the applications that devices run. The Software license monitoring window shows Macintosh applications along with Windows applications. You can deny Macintosh application execution in the same manner by adding Macintosh applications to the To be denied list.

Macintosh applications don't come prebundled in the LDAPPL3.INI file. You will have to set the LDAPPL3 file mode to "all" or "unlisted" first so that Macintosh applications are in the database to be dispositioned. When you think that all of the Macintosh applications are included, you can then set the mode back to "listed."

Macintosh devices can use the LANDesk Client pane's Software license monitoring tab (from **System Preferences**) to show what applications are installed and how often they have been used. This tab also shows blocked applications that won't launch on the device.

Security and Patch Manager for Macintosh devices

Security and Patch Manager is a complete, integrated security solution that helps you protect your Macintosh devices from a wide range of prevalent security risks. The tool allows you to manage security and patch content, scan devices, use patches, and remediate devices.

Note: Security and patch manager only supports Mac OS X devices.

Configuring Macintosh devices for security scanning and remediation

Before Macintosh devices can be scanned for vulnerabilities, spyware, security threats, and other security types, and receive patch deployments or software updates, they must have the Security and Patch manager agent installed. The Security and Patch manager agent is part of the standard LANDesk agent for Macintosh devices. If vulnerabilities are detected, remediation must be performed on the affected device.

For more information on creating and deploying a Macintosh agent configuration with security and patch manager support, see Agent Configuration for Macintosh devices.

Launching the scanner for Macintosh devices

You can launch the scanner from the console or manually on the client machine.

To launch the security scanner

1. Open the Mac OS X **System Preferences** on the target device and select the **LANDesk Client** panel.
2. On the **Overview** tab, click **Check Now** in the Security and Patch Manager section.

Managing a client Macintosh machine

From a Macintosh client machine, you can manage LANDesk services running on the device, as well as perform general administrative tasks like creating new users, locking/unlocking the client machine configuration, logging in as a different user, and uninstalling LANDesk agents.

System requirements

Your computer needs to meet or exceed the following system requirements:

- Power Macintosh, Power Mac, PowerBook, iMac, eMac, or iBook with a G3 processor or better, at 400 MHz or faster
- Mac OS X version 10.2 or later
- 128 megabytes (MB) of physical random-access memory (RAM)
- 5 megabytes (MB) of free hard disk space

Managing LANDesk services on a Macintosh machine

The LANDesk Client dialog in System Preferences is used to manage the LANDesk services on Macintosh devices (**System Preferences | LANDesk Client**). Configuring the services defines how the server will interact with the device.

The dialog enables you to specify the LDMS (core) server address. You can lock the dialog to prevent other users from making changes to the device's configuration.

The LANDesk Client dialog consists of the following tabs:

- Overview
- Policy-based distribution
- Inventory scanner
- Remote control
- Software license monitoring

Overview

The Overview page provides status and usage information for services running on the device. From this page, you can also check policy-based distribution, start the inventory scanner, or check patch management.

Policy-based distribution

The Policy-based distribution page lists the policies that are installed on the device and the dates they were installed.

Inventory scanner

The Inventory scanner page enables you to configure how the device will interact with the server during an inventory scan.

The page consists of the following options:

- **Send scan to LDMS server:** Sends data collected from the scan to the core server.
- **Save scan in directory:** Sends data collected from the scan to the specified directory.
- **Choose scan components:** Specifies which components the inventory scanner will collect data on.
- **Force software scan:** Forces a software scan to be done whenever a hardware scan is conducted.
- **Scan applications folder only:** Restricts the hardware scan and runs the software scan.

Remote control

The Remote control page enables you to configure what users can do when they take control of the device.

The page consists of the following options:

- **Allow user to do the following to this computer:** Specifies what the user is able to do if they take control of the device, such as opening applications and files, copying items, deleting and renaming items, locking the keyboard and mouse, blanking the screen, restarting and shutting down the computer, and controlling and observing the device, including showing the device when it's being observed.
- **Give control to user:** Species the category that a user must belong to in order to gain control of the device.

Software license monitoring

The Software license monitoring page lists the applications that are running on the device, how many times each application has launched, how many time the application has been denied, and the duration the applications have been running. It also contains a list of all applications to be denied.

Using Security and Patch Manager

LANDesk Security and Patch Manager is a complete, integrated security solution that helps you protect your managed devices from a wide range of prevalent security risks.

Security and Patch Manager provides all the tools you need in order to: update the most common types of security and patch content (such as vulnerabilities, spyware, configuration security threats, and unauthorized applications) from LANDesk Security services, download the required patches, and configure and run security assessment and remediation scans on your LANDesk managed devices. You can also create your own custom definitions. If any security risks are detected, you can use Security and Patch Manager to remediate the affected devices. At any time, you can view detailed security and patch information for scanned devices, and generate specialized security and patch reports. All of these security management tasks can be performed from the convenience of the console.

Additionally, Security and Patch Manager lets you scan managed devices, and core servers and console machines, for versions of installed LANDesk software and deploy the appropriate LANDesk software updates.

About the LANDesk Security Suite

The Security and Patch Manager tool is the main security management component of the LANDesk Security Suite product. The Security Suite is based on much of the primary LANDesk Management Suite functionality, supplemented with specialized security management tools such as the Security and Patch Manager and connection control manager. The Security and Patch Manager tool itself is identical in both Management Suite and Security Suite, and is described in detail in this chapter. For more information on which basic LANDesk functionality is supported in the Security Suite product, see Using LANDesk Security Suite.

About endpoint compliance security and the new LANDesk Trusted Access tool

Endpoint compliance security is now available for your LANDesk network with the new LANDesk Trusted Access tool. LANDesk Trusted Access, in conjunction with the custom policy, scanning, and remediation capabilities of Security and Patch Manager, enables you to control access to the corporate network by verifying the health of connecting devices, blocking and/or remediating infected devices, and protecting the network from malicious intrusion. LANDesk Trusted Access adds another powerful layer of security to your LANDesk network. For more information on how to set up and use a LANDesk trusted access solution, see Using LANDesk trusted access.

Read this chapter to learn about:

Security and Patch Manager overview

- Security and Patch Manager overview
- Security content types
- Supported device platforms
- Role-based administration with Security and Patch Manager
- Understanding and using the Security and Patch Manager window
- Security and patch management workflow
- Configuring devices for security scanning and remediation

What you should do after configuring devices for security scanning

Once you understand the Security and Patch Manager concepts, the tool interface, general tasks and workflow, and have configured devices for security scanning and remediation, you can then perform the following security management tasks: updating and viewing security content, downloading patches, creating custom vulnerability definitions, scanning managed devices for a variety of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.), remediating affected devices, as well as generating security alerts, logging, and reports. For information on performing these tasks, see [Managing security content and patches](#), and [Scanning and remediating devices](#).

Security and Patch Manager overview

Security and Patch Manager provides all of the tools you need to establish strong system security across your network. With Security and Patch Manager, you can automate the repetitive processes of maintaining security and patch content, and organizing and viewing that content.

You can use security scan tasks and policies to assess managed devices for known platform-specific vulnerabilities. You can download and manage patch executable files. Finally, you can remediate detected vulnerabilities by deploying and installing the necessary patch files, and verify successful remediation.

Additionally, you can create your own custom vulnerability definitions in order to scan managed devices for specific OS and application conditions that might threaten the operation and security of your system. Custom definitions can be configured for detection only or for both detection and remediation. For more information, see [Creating custom definitions and detection rules](#).

New security scanning and remediation capabilities

Security and Patch Manager has added several scanning and remediation capabilities. For example, you can now:

- Scan for the presence of spyware on your managed devices. If spyware is detected on a device, you can schedule a repair job that removes the spyware from affected devices.
- You can also deny launch of unauthorized or prohibited applications on end user devices with blocked application definitions.
- Enable real-time spyware monitoring (detection and removal), and real-time application blocking.
- You can scan managed devices for security threats (Windows system configuration errors and exposures) on the local hard drive. Once a security threat is identified, you can perform the necessary fix manually at the affected device.
- One of the available security threat definitions lets you detect some firewalls, turn them on or off, and configure firewall settings.
- Use custom variables that are included with other security threat definitions in order to customize system configurations and establish enterprise-wide system configuration policies.
- Scan for third-party antivirus scanners, enable real-time virus scanning, and ensure up-to-date antivirus pattern files.
- Receive alerts when specified vulnerabilities are detected on managed devices by a security scan. You can configure alerting by vulnerability type or severity.
- Implement frequent security scans for critical, time-sensitive security risks such as virus scanning.
- Enforce endpoint security and compliance security policies with the Compliance group and the new LANDesk Trusted Access tool.
- Use vulnerability dependency relationships to identify which patches need to be installed before other vulnerabilities can adversely affect managed devices or before they can be remediated. Supersedence information can inform you of patches that have been replaced by more recent versions and that don't need to be applied.

- Verify the latest LANDesk software is installed on your managed devices, as well as core servers and console machines, by scanning for LANDesk software updates. If an outdated version is detected on a device, you can schedule a repair job that deploys and installs the latest LANDesk software update.

Additional features and benefits

With Security and Patch Manager, you can:

- Provide patch security for international versions of the operating systems on your network, including current support for the following languages: Czech, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Portuguese, Simplified Chinese, Spanish, Swedish, and Traditional Chinese.
- Organize and group security definitions to perform customized security assessment and remediation.
- Assess vulnerabilities and other security risks on a variety of supported device platforms, including Windows, Sun Solaris, and Linux.
- View security and patch information for scanned devices.
- Schedule automatic patch management tasks, including content updates, device scans, and patch downloads.
- Perform remediation as a scheduled task, a policy, or automatically with the Auto Fix feature.
- Download, deploy, and install patches that have been researched and verified.
- Track the status of patch deployments and installation on scanned devices.
- Use LANDesk's Targeted Multicast, peer download, and checkpoint restart features for fast and efficient patch deployment.
- Generate and view detected an extensive variety of security and patch management-specific reports.

Security content types and subscriptions

When you install LANDesk Management Suite, the Security and Patch Manager tool is now included by default (previously, it was a separate add-on). However, without a Security Suite content subscription, you can only scan for LANDesk software updates and custom definitions. A Security Suite content subscription enables you to take full advantage of the Security and Patch Manager tool by providing access to additional security and patch content (definition) types.

LANDesk Security Suite content types include:

- Antivirus
- Blocked applications
- Custom vulnerability definitions
- Driver updates
- LANDesk software updates
- Security threats (system configuration risks and exposures; includes firewall detection and configuration)
- Software updates
- Spyware
- Vulnerabilities (known platform and application specific vulnerabilities)

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

Scanning and remediation functions are not the same between these content types. For more information, see the appropriate sections below.

Supported device platforms

Security and Patch Manager supports most of the standard LANDesk-managed device platforms, including the following operating systems:

- Windows 98 SE
- Windows NT (4.0 SP6a and higher)
- Windows 2000 SP4 / 2003 / XP SP1
- Mac OS X 10.2.x and 10.3.x
- Red Hat Linux, version 9 (scanning from the console, manual remediation)
- SUSE Linux (scanning from the console, manual remediation)
- Sun Solaris (scanning from the console, manual remediation)

For information on configuring managed devices for security and patch scanning, see Configuring devices for security scanning and remediation later in this chapter.

Scanning core servers and consoles for LANDesk software updates is supported

You can also scan LANDesk core servers and consoles for LANDesk software updates, but they must first have the standard LANDesk agent deployed, which includes the Security and patch scanner agent required for security scanning tasks.

Role-based administration with Security and Patch Manager

Security and Patch Manager uses LANDesk's role-based administration to allow users access to the Security and Patch Manager features. Role-based administration is LANDesk's access and security framework that lets LANDesk Administrators restrict user access to tools and devices. Each LANDesk user is assigned specific rights and scope that determine which features they can use and which devices they can manage. For more information about role-based administration, see Using role-based administration.

A LANDesk Administrator assigns these rights to other users with the Users tool in the console. Security and Patch Manager introduces one new role and corresponding right to role-based administration. The right is called Security and Patch Manager, and it appears in the User Properties dialog. In order to see and use this tool, a LANDesk user must be assigned the necessary Security and Patch Manager right.

Security and Patch Manager rights

Security and Patch Manager is controlled by two role-based administration rights, as described below:

Security and Patch Manager

- The Security and Patch Manager right provides users the ability to:
- See and access the Security and Patch Manager tool in the Tools menu and Toolbox
- Configure managed devices for security assessment and remediation scanning
- Configure devices for real-time spyware and blocked application scanning

- Configure devices for high frequency scanning for critical security risks
- Download security updates (definitions and detection rules) and associated patches for the security types for which you have a Security Suite content subscription
- Create scheduled tasks that automatically download definitions and/or patch updates
- Create custom vulnerability definitions and custom detection rules
- Import, export, and delete custom definitions
- View downloaded security and patch content by type (including: all types, blocked applications, custom definitions, LANDesk updates, security threats, spyware, vulnerabilities, driver updates, and software updates)
- Customize selected security threats with custom variables
- Configure and run security scans on managed devices as a scheduled task or as a policy
- Divide a scheduled task scan into a staging phase and a deployment phase
- Create and configure scan and repair settings that determine the scan options, such as: content type to be scanned for, scanner information and progress display, device reboot behavior, and the amount of end user interaction. Then, apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks
- View detailed scan results (detected security data) by: detected group, specific definition, individual device, or a group of selected devices
- Perform remediation as a scheduled task or as a policy
- Use Auto Fix to automatically remediate the following security types if they are detected: vulnerabilities, spyware, LANDesk software updates, and custom definitions (must be a LANDesk Administrator)
- Track and verify the status of patch deployment and installation (repair history) on scanned devices
- Purge unused security type definitions (must be a LANDesk Administrator)
- Uninstall patches from scanned devices
- Remove patches from the core database
- Configure vulnerability alerts
- Generate a variety of security specific reports (also requires the Reports right)
- Much more...

Security and Patch Compliance

The Security and Patch Compliance right provides users the ability to:

- Add and remove security definitions from the Compliance group
- Change the status of definitions contained in the Compliance group
- Cannot edit custom definitions or security threat's custom variables
- Cannot configure trusted access services, such as adding posture servers or remediation servers, or configure and publish compliance rules (must be a LANDesk Administrator)

Understanding and using the Security and Patch Manager window

The Security and Patch Manager window, like all other LANDesk tool windows, is opened from either the Tools menu or the Toolbox and can be docked, floated, and tabbed with other open tool windows (see "Dockable windows"). Note that with LANDesk's role-based administration, a LANDesk user must have either the LANDesk Administrator right (implying full rights), or the specific Security and Patch Manager right, to be able to see and access the Security and Patch Manager tool. For more information on user rights and scope, see "Using role-based administration."

The Security and Patch Manager window contains a toolbar and two panes. The left-hand pane shows a hierarchical tree view of security type definition and detection rule groups. You can expand or collapse the objects as needed. The right-hand pane displays a column list of the selected group's definition details or detection rule details, depending upon which group you've selected in the left-hand pane.

The Security and Patch Manager window includes a toolbar with the following buttons:

Toolbar buttons

- **Download updates:** Opens a dialog where you can specify the platforms and languages for the content types you want to update, as well as which LANDesk Security content server to access. You can also configure whether to place definitions in the Unassigned group, whether to download associated patches concurrently, the location where patches are downloaded, and proxy server settings.
- **Schedule download:** Creates a Download Security and Patch Content task that appears in the Scheduled Tasks window where you can configure scheduling options.
- **Create a task:** Includes a drop-down list where you can select which type of task you want to create: security scan task, reboot task, repair task, or to gather historical information.
 - The **Security scan** task opens a dialog where you can enter a name for the scan, specify whether the scan is a scheduled task or a policy, and select a scan and repair setting that determines whether the security scanner displays, reboot and interaction behavior, and the content types scanned for.
 - The **Reboot task** opens a dialog where you can enter a name, specify whether the reboot is a scheduled task or a policy, and select a scan and repair setting that determines display and interaction behavior.
 - The **Repair** task opens a dialog where you can configure the repair as a scheduled task or as a policy or both, divide the repair task into separate staging and repairing phases, select a scan and repair settings, and download patches.
 - The **Gather historical information** task opens a dialog that lets you gather the current scanned and detected counts (for a specified number of days) that can be used for reporting, or create and configure a scheduled task that performs the same process.
- **Computers out of compliance:** Lists devices that have been scanned to check for compliance with the predefined compliance security policy (based on the content of the Compliance group, and the definition of healthy found on the Configured trusted access dialog), and are determined to be unhealthy or out of compliance.
- **Configure scan and repair settings:** Opens a dialog where you can create, edit, apply, and delete scan and repair settings.
- **Refresh:** Updates the contents of the selected group.

- **Create custom definition:** Opens a blank Definition properties dialog with editable fields where you can specify whether the custom definition is detection only or also allows remediation, enter specific vulnerability information, create detection rules, and identify the appropriate patch file for remediation.
- **Import custom definitions:** Allows you to import an XML file containing definitions.
- **Export selected custom definitions:** Allows you to export a custom definition as an XML file.
- **Delete selected custom definitions:** Removes the selected custom definitions from the core database.
- **Purge security and patch definitions:** Opens a dialog where you can specify the platforms and languages whose definitions you want to remove from the core database. Note that only a LANDesk Administrator user can perform this operation.
- **Publish trusted access settings:** Opens a dialog that lets you specify which information you want to publish to posture validation servers and remediation servers. Trusted access content (security definitions and compliance criteria) is published to posture validation servers. Infrastructure files (the security scanner, relevant patches, and the HTML pages) are published to remediation servers. For more information, see the LANDesk trusted access chapter.
- **Help:** Opens the online help, to the Security and Patch Manager section.

Type drop-down list

Use the **Type** drop-down list to determine which definitions display in the tree view.

The **Type** drop-down list includes the following options:

- All types
- Antivirus
- Blocked applications
- Custom definitions
- Driver updates
- LANDesk updates
- Security threats
- Software updates
- Spyware
- Vulnerabilities

The left pane of the Security and Patch Manager window shows the following items:

Security and Patch Manager

Security and Patch Manager is the root object of the Security and Patch Manager tree, containing all of the security types such as vulnerabilities, spyware, security threats, blocked applications, and custom definitions groups (and associated detection rule groups, if applicable). The root object can be expanded and collapsed as needed.

Type name (or All Types)

The type groups contain the following subgroups:

- **Detected:** Lists all of the definitions detected by security scans, for all of the devices included in the scans. The contents of this group are cumulative based on all the security scans run on your network. Definitions are removed from this group only by: being successfully remediated, being removed from the Scan group and running the scan again, or by actually removing the affected device from the database.

The Detected list is a composite of all detected security definitions found by the most recent scan. The Scanned and Detected columns are useful in showing how many devices were scanned, and on how many of those devices the definition was detected. To see specifically which devices have a detected definition, right-click the item and click **Affected computers**.

Note that you can also view device-specific information by right-clicking a device in the network view, and then clicking **Security and Patch Information**.

You can only move definitions from the Detected group into either the Unassigned or Don't Scan groups.

- **Scan:** (For Blocked Applications, this group is called **Block**) Lists all of the security definitions that are searched for when the security scanner runs on managed devices. In other words, if a definition is included in this group, it will be part of the next scan operation; otherwise, it won't be part of the scan.

By default, collected definitions are added to the Scan group during a content update.

(Important: Except for blocked applications, which are added to the Unassigned group by default.)

Scan can be considered one of three possible states for a security definition, along with Don't Scan and Unassigned. As such, a definition can reside in only one of these three groups at a time. A definition is either a Scan, Don't Scan, or Unassigned and is identified by a unique icon for each state (question mark (?) icon for Unassigned, red X icon for Don't Scan, and the regular vulnerability icon for Scan). Moving a definition from one group to another automatically changes its state.

By moving definitions into the Scan group (click-and-drag one or more from another group, except from the Detected group), you can control the specific nature and size of the next security scan on target devices.

Caution about moving definitions from the Scan group

When you move definitions from the Scan to the Don't Scan group, the current information in the core database about which scanned devices detected those definitions is removed from the core database and is no longer available in either an item's Properties dialog or in a device's Security and Patch Information dialog. To restore that security assessment information, you would have to move the definitions back into the Scan group and run the same security scan again.

- **Don't Scan:** (For Blocked Applications, this group is called **Don't Block**) Lists all of the definitions that aren't searched for the next time the security scanner runs on devices. As mentioned above, if a definition is in this group, it can't be in the Scan or Unassigned group. You can move definitions into this group in order to temporarily remove them from a security scan.
- **Unassigned:** Lists all of the definitions that do not belong to either the Scan or Don't Scan groups. The Unassigned group is essentially a holding area for collected definitions until you decide whether you want to scan for them or not.

You can move definitions (click-and-drag one or more) from the Unassigned group into either the Scan or Don't Scan groups.

New definitions can also be automatically added to the Unassigned group during a content update by checking the **Put new definitions in the Unassigned group** option on the **Download updates** dialog.

- **All Items:** Lists all of the selected type's definitions in a flat list, even if you've moved a definition into either the Unassigned, Scan, or Don't Scan group.
- **View by Product:** Lists all of the definitions organized into specific product subgroups. These subgroups help you identify definitions by their relevant product category.

You can use these product subgroups to copy definitions into the Scan group for product-specific scanning, or copy them into a custom group (see below) in order to perform remediation for groups of products at once.

Definitions can be copied from a product group into the Scan, Don't Scan, or Unassigned group, or any of the user-defined custom groups. They can reside in platform, product, and multiple custom groups simultaneously.

Detection Rules

Note: Detection rules define the specific operating system, application, file, or registry conditions that a definition checks for in order to detect the applicable security risk (vulnerabilities, custom definitions, and security threats) on scanned devices. Spyware and blocked applications do not apply.

The Detection Rules group contains the following subgroups:

- **Scan:** Lists all of the detection rules that are enabled for security scanning on devices.

By default, detection rules associated with a definition of any security content type are added to the Detection Rules Scan group during a content update. Likewise, custom detection rules associated with a custom definitions are added to the Scan group when you create the custom definition.

Note that in addition to having a definition's detection rules enabled, its corresponding patch executable file must also be downloaded to a local patch repository on your network (typically the core server) before remediation can take place. The Downloaded attribute (one of the detail columns in the tool window's right-hand pane) indicates whether the patch associated with that rule has been downloaded.

- **Don't Scan:** Lists all of the detection rules that are disabled for security scanning on devices. Some definitions have more than one detection rule. By disabling a detection rule, you can ensure that it won't be used to scan for the conditions indicating that definition is present on devices. This can allow you to simplify a security scan without redefining the definition.
- **View by Product:** Lists all of the detection rules for collected definitions, organized into specific product subgroups. These subgroups help you identify detection rules by their relevant product category.

You can use these product subgroups to perform group operations.

Groups

Contains the following subgroups:

- **My Groups:** Lists all of the subgroups you've created and the definitions they contain. My Groups provide a way for you to organize security definitions however you want. Use a group's contents to copy several definitions into the Scan group for customized scanning, or to create a repair job for several definitions at once.

You can also use a custom group to define the contents of a security scan. Copy the definitions you want to scan for into a custom group and select that group in the Scan for option of the Scan and repair settings dialog.

To create a custom group, right-click **My Groups** (or a subgroup) and then click **New Group**.

To add definitions to a custom group, click-and-drag one or more of them from any of the other definition groups. Or, you can right-click a custom group, and then click **Add Definition**.

- **Alert:** Lists all of the definitions that will generate an alert message the next time the security scanner run on devices. For more information, see Using vulnerability alerts.
- **Compliance:** Lists all of the definitions that are used to determine whether a managed (or mobile/guest) device is Healthy or Unhealthy. This group is used by the new LANDesk Trusted Access feature to deny or allow access to the main network. The definitions and associated patch files contained in the Compliance group are copied to a special remediation server that scans devices, determines compliance or non-compliance (according to compliance rules published to a posture server), and can remediate non-compliant devices so that they can be granted full access to the corporate network.

Trusted Access

The trusted access group contains the follows items:

- **Posture server logs:** Lists the policy server logs. Also, you can right-click this object in order to access the Configure trusted access dialog where you can add posture servers and remediation servers to the network, configure compliance rules, as well as configure compliance logging.

The right pane of the Security and Patch Manager window displays detailed information listed in sortable columns for definition and detection rule items, as described below:

Definition details

- **ID:** Identifies the definition with a unique, vendor-defined alphanumeric code.
- **Severity:** Indicates the severity level of the definition. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown.
- **Title:** Describes the nature or target of the definition in a brief text string.
- **Language:** Indicates the language of the OS or application affected by the definition.
- **Date Published:** Indicates the date the definition was published by the vendor.
- **Repairable:** Indicates whether the definition can be repaired through patch file deployment and installation. Possible values are: Yes, No, Some (for a definition that includes multiple detection rules and not all detected definitions can be fixed), and No rules (for a custom definition that doesn't include any detection rules).
- **Silent Install:** Indicates whether the definition's associated patch (or patches) installs silently on devices (without user interaction), with a Yes or No. Some definitions may have more than one patch. If any of a definition's patches don't install silently, the Silent Install attribute says No. To see how individual patches install, right-click the definition and click **Properties | Patches**.
- **Detected:** Displays the number of scanned devices that detected the definition.

- **Scanned:** Displays the number of devices scanned for the definition.
- **Auto Fix:** Indicates whether Auto Fix is enabled or disabled for the definition.

Right-click an item to view more details with the Properties option. The shortcut menu also lets you view affected computers, enable/disable Auto Fix, clear scan information and repair status, and create a repair job.

Detection Rule details

- **Name:** Displays the name of the detection rule (can be the file name of the patch executable).
- **ID:** Displays the ID of the definition associated with the rule.
- **Repairable:** Indicates whether the associated definition can be repaired through patch file deployment and installation.
- **Silent Install:** Indicates whether the rule's associated patch installs silently on devices (without user interaction), with a Yes or No.
- **Reboot:** Indicates whether the associated patch file requires a system reboot in order to complete a successful remediation.
- **Auto Fix:** Indicates whether Auto Fix is enabled or disabled for the associated definition.
- **Downloaded:** Indicates whether the rule's associated patch executable file has been downloaded to the local repository.

Right-click a detection rule to view more details with the **Properties** option. The shortcut menu also lets you enable/disable the rule and download the associated patch.

Security and patch management workflow

The following steps provide a quick summary outline of the typical processes involved in implementing security and patch management on your LANDesk network.

All of these procedures are described in detail in subsequent sections.

Basic workflow steps

1. Configuring managed devices for security scans and remediation.
2. Collecting updated security and patch information from industry/vendor data sources. Also, creating custom definitions.
3. Organizing and viewing security and patch information.
4. Creating and configuring scan tasks and policies. Scan for vulnerabilities, spyware, security threats, blocked applications, etc.
5. Viewing scan results for scanned devices.
6. Downloading patches for detected vulnerabilities
7. Repairing detected vulnerabilities by deploying and installing patches to affected devices
8. Repairing other detected definition types.
9. Viewing patch installation status and repair history information.

Configuring devices for security scanning and remediation

Before managed devices can be scanned for vulnerabilities, spyware, security threats, and other security types, and receive patch deployments or software updates, they must have the Security and patch scanner agent installed.

This section includes information about configuring Windows devices as well as Linux, UNIX and Mac devices.

Scanning core servers and consoles for LANDesk software updates is supported

You can also scan LANDesk core servers and consoles for LANDesk software updates, but they must first have the standard LANDesk agent deployed, which includes the Security and patch scanner agent required for security scanning tasks.

Configuring Windows devices for security scanning

With previous versions, for Windows devices, the vulnerability scanner agent had to be installed as a separate add-on component to an existing device agent configuration.

However, now the security and patch scanner agent is included by default with the standard LANDesk agent and is installed on devices with even the most basic agent configuration. In other words, any Windows device configured with the new Agent configuration tool will be ready for security and patch scanning and remediation.

Configuring scan and repair options for Windows devices during agent configuration

When creating or editing an agent configuration, you can specify some of the security and patch scanner's options, such as when and how often the scanner runs automatically on managed devices, whether the scanner displays progress and prompts on the end user device, as well as global settings for remediation operations such as device reboot and autofix. For more information on customizing the behavior of the security and patch scanner agent as part of creating and deploying agent configurations to managed Windows devices, see About the Agent configuration dialog's Security and patch scan page.

Note: WinSock2 is required on Windows 9x devices in order for the Vulnerability Scanner agent to run.

After agent configuration occurs, a program icon for the security and patch scanner is added to the device's LANDesk Management program group, that can be used to run the scanner directly from the device (as opposed to any runkey launch, recurring local scheduler launch, or scheduled task using the console).

Additional security settings in agent configurations

When defining a device agent configuration (for Windows devices), you can also enable and configure the following the security scanner settings:

- Frequent security scanning for critical security risks
- Real-time application blocker and spyware monitoring

See the sections below for more information.

About the Agent configuration dialog's Frequent security scan page

Use this page to enable and configure high frequency scanning for critical, time-sensitive security risks such as recently discovered and malignant viruses, and firewall configuration risks.

- **Use the frequent security scanner:** Enables high frequency scanning with the security and patch scanner, based on the time and group content specified below. If this option is not selected, managed devices configured with this agent configuration will still be able to be scanned with the security and patch scanner, according to the settings specified on the Security and patch scan page (because the security and patch agent is part of the standard LANDesk agent).
- **Scan only when a user is logged in, every:** Specifies how often the frequent security scan runs when a user is logged in to a managed device. The minimum frequency is 30 minutes.
- **Choose a scan and repair setting:** Determines the security type's definitions that are scanned by the high frequency scan, based on the contents of the custom group selected here. The high frequency scan can only be defined by the contents of a custom group, not the Scan, Alerts, or Compliance groups. (Any type of security content type can be added to a custom group, such as spyware, vulnerabilities, custom definitions, security threats, etc.) The custom group is selected on the scan and repair settings dialog. Choose a scan and repair setting from the drop-down list. Only scan and repair settings that are configured to scan for a custom group (as opposed to a specific type or types) appear in this list.
- **Configure:** Opens the scan and repair settings dialog where you can select a scan and repair setting that has a custom group scan specified.

About the Agent configuration dialog's Spyware/Application blocker page

Use this page to enable and configure real-time application blocking and spyware detection and removal on managed devices configured with this agent configuration.

- **Allow application blocking monitoring:** Enables real-time application blocking, based on the list of unauthorized applications (definitions) contained in the Scan group (or custom group).
 - **Notify user when and application has been blocked:** Displays a message on the end user device notifying them that the application they attempted to launch has been denied or blocked.
- **Allow real-time spyware monitoring:** Enables real-time spyware detection and removal, based on the list of spyware definitions contained in the Scan group (or custom group).

Important: In order for real-time spyware scanning and detection to work, you must manually enable the autofix feature for any downloaded spyware definitions you want included in a security scan. Downloaded spyware definitions don't have autofix turned on by default.

- **Notify user when spyware has been blocked:** Displays a message on the end user device notifying them that known spyware has been detected and removed from their system.

- **Prompt user when an unknown application is being installed:** Displays a message on the end user device notifying them that an unknown application is being installed on their system.

Configuring Linux and UNIX devices for security scanning

Security and Patch Manager also supports vulnerability scanning on:

- Red Hat Linux
- SUSE Linux
- Sun Sparc (Solaris 8)

Each of these platform's security and patch content can be downloaded with Security and Patch Manager just as with Windows vulnerabilities.

Linux and UNIX devices can't be configured with the security and patch scanner agent via the console's agent configuration tool. Linux and UNIX device configuration is a manual process. For more information on setting up Linux and UNIX devices, see the *Installation and Deployment Guide*, as well as the README file contained in the respective platform's tar file located in the platforms folder under ManagementSuite\LDLogon on the core server.

Once configured, these Linux and UNIX platforms can be scanned for vulnerabilities via scheduled tasks from the console. If vulnerabilities are detected, remediation must be performed manually at the affected device.

Configuring Mac OS X devices for security scanning

On Macintosh OS X devices, Security and Patch Manager now supports both security scanning and remediation. Macintosh security and patch content can be downloaded with Security and Patch Manager.

Additionally, you can create and configure agent configuration for your Macintosh devices with the Agent configuration tool. As with Windows agent configuration, the security and patch scanner agent is part of the default standard LANDesk agent for Macintosh devices. To create and deploy a Macintosh agent configuration with security and patch scanner support, see "Working with Macintosh devices" in the *Users Guide*.

Once configured, Macintosh devices can be scanned for vulnerabilities via scheduled tasks from the console. If vulnerabilities are detected, remediation must be performed at the affected device.

To launch the security scanner manually on Mac devices

1. Open the Mac OS X **System Preferences** and select the **LANDesk Client** panel.
2. On the **Overview** tab, click **Check Now** in the Security and Patch Manager section.

Legal disclaimer for the blocked applications type

As a convenience to its end users, LANDesk provides access to a database containing certain information regarding executable files that an end user may utilize in connection with the application blocker functionality of the LANDesk® Security Suite. THIS INFORMATION IS PROVIDED AS-IS WITHOUT ANY EXPRESS, IMPLIED, OR OTHER WARRANTY OF ANY KIND, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. As such, LANDesk does not guarantee the accuracy, completeness or currency of this information and the end user is responsible to review and confirm this information before use. Any use of this information is at the end users own risk.

This chapter provides information on updating and viewing security content, creating and using custom definitions, and downloading and working with patches.

For information on actually scanning managed devices for a variety of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.), remediating affected devices, as well as generating security alerts, logging, and reports, see *Scanning and remediating devices*.

Read this chapter to learn about:

Managing security content

- Updating security and patch content
- Viewing security and patch content
- Using filters to customize item lists
- Purging unused definitions

Managing custom definitions

- Creating custom definitions and detection rules
- Importing and exporting custom definitions
- Deleting custom definitions

Managing patches

- Downloading patches
- Uninstalling patches
- Removing patches from the core database

Updating security and patch content

Your network is continuously vulnerable to security risks from worms, viruses, spyware, as well as ordinary maintenance issues like software updates and bug fixes. Patches are released regularly to repair inevitable operating system and application vulnerabilities. Security and Patch Manager makes the process of gathering the latest security type's definitions and patches quick and easy by letting you download content via a LANDesk-hosted database. This LANDesk Security service consolidates known definitions from trusted, industry/vendor sources and sends reliable information directly to you.

Security and Patch Manager also supports custom vulnerability definitions

In addition to known vulnerabilities, you can also create your own custom vulnerability definitions and associated detection rules. For more information, see [Creating custom definition and detection rules](#) later in this chapter.

By establishing and maintaining up-to-date security and patch content, you can better understand the nature and extent of the security risks for each platform and application you support, determine which vulnerabilities and other types of risks are relevant to your environment, and customize security scanning and remediation tasks. The first step in this security management strategy is to download a current listing of the latest known security and patch content.

With Security and Patch Manager, you can configure and perform security and patch content updates at once, or create a scheduled update task to occur at a set time or as a recurring task (see [Scheduling automatic security and patch content updates](#) later in this chapter).

Only one LANDesk user on a specific core server (including additional consoles) can update security and patch content at a time. If a user attempts to update content while the process is already running, a message prompt appears indicating there is a conflict.

To update security and patch content

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Download updates** toolbar button.
3. Select the update source site from the list of available content servers.
4. Select the definition types whose security and patch content you want to update. You can select one or more types in the list (depending on your LANDesk Security Suite content subscription). The more types you select, the longer the update will take.
5. Select the languages whose content you want to update for the types you've specified.

Some vulnerability and other definition types, and any associated patches, are language neutral or independent, meaning they are compatible with any language version of the OS or application addressed by that definition. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages. For example, Linux and UNIX platforms use only language neutral definitions and patches. However, Microsoft Windows and Apple Macintosh platform vulnerability definitions and patches are nearly always language specific.

When downloading content for any platform (with the appropriate subscription), all of the selected platform's language neutral vulnerability definitions are automatically updated by default. If you've selected a Windows or Mac content type, you must also select the specific languages whose definitions you want to update. If you've selected the Sun Solaris or a Linux platform, you do not have to select a specific language because their content is language neutral and will be updated automatically.

6. If you want new content (content that does not already reside in any groups in the Security and Patch Manager tree) to automatically be placed in the Unassigned group instead of the default location, which is the Scan group, check the **Put new definitions in the Unassigned group** check box.
7. If you want to automatically download associated patch executable files, click the **Download patches** check box, and then click one of the download options:
 - **For detected definitions only:** Downloads only the patches associated with vulnerabilities, security threats, or LANDesk updates detected by the last security scan (i.e., the definitions that are currently residing in the Detected group).
 - **For all downloaded definitions:** Downloads ALL of the patches associated with vulnerability, security threats, and LANDesk updates currently residing in the Scan group.

Patches are downloaded to the location specified on the **Patch Location** tab of the Download updates dialog.

8. If you have a proxy server on your network that is used for external Internet transmissions (that is required to update security and patch content and download patches), click the **Proxy Settings** tab and specify the server's address, port number, and authentication credentials if a login is required to access the proxy server.
9. Click **Apply** from any of the tabs at any time to save your settings.
10. Click **Update Now** to run the security and patch content update. The **Updating Definitions** dialog displays the current operation and status.
11. When the update has completed, click **Close**. Note that if you click **Cancel** before the update is finished, only the security and patch security content that has been processed to that point is downloaded to the core database. You would need to run the update again in order to obtain all of the remaining security and patch content.

Note: Do not close the console while an update security and patch process is running or the process will be terminated. However, this rule does not apply to a Download Security and Patch Content scheduled task, which will finish processing even if the console is closed while it is running.

To configure the patch download location

1. On the **Download updates** dialog, click the **Patch Location** tab.
2. Enter a UNC path where you want the patch files copied. The default location is the core server's \LDLogon\Patch directory.
3. If the UNC path entered above is to a location other than the core server, enter a valid username and password to authenticate to that location.
4. Enter a Web URL where devices can access the downloaded patches for deployment. This Web URL should match the UNC path above.
5. You can click **Test Settings** to check to see if a connection can be made to the Web address specified above.
6. If you want to restore the UNC path and Web URL to their default locations, click **Restore to Default**. Again, the default storage location is the core server's \LDLogon\Patch directory.

Scheduling automatic security and patch content updates

You can also configure security and patch content updates as a scheduled task to occur at a set time in the future, or as a recurring task. To do this, simply click the **Schedule download** toolbar button to create an Download Security and Patch Content task in the Scheduled Tasks window, and then set the schedule options.

All scheduled Download Security and Patch Content tasks will use the current settings found in the Download updates dialog. So, if you want to change the content types, platforms, languages, patch download location, or proxy server settings for a particular update job, you must first change those settings in the Download updates dialog BEFORE the task is scheduled to run.

Viewing security and patch content

After security and patch content has been updated with the LANDesk Security service, you can view the definitions and detection rules (for vulnerabilities and custom definitions only) in their respective groups in the Security and Patch Manager window.

Use the **Type** drop-down list to view content for a specific type or for all types. You can also use the **Filter** control to further customize the content you want to display.

Once security and patch content has been downloaded, you can move items into different status groups, or copy them into your own custom groups. For information on how to use the different groups in the Security and Patch Manager view, see Understanding the Security and Patch Manager window earlier in this chapter.

You can also view property details for each of the updated definitions and detection rules by right-clicking an item and selecting **Properties**. This information can help you determine which definitions are relevant to your network's supported platforms and applications, how detection rules check for the presence of definitions, what patches are available, and how you want to configure and perform remediation for affected devices.

Custom definitions can be modified

If you select a downloaded industry definition, its properties dialog is primarily for information viewing purposes only. However, if you select a custom definition, or are creating a new custom definition, the pages and fields in the properties dialog are editable, allowing you to define the definition and its detection rules.

You can also view information specific to scanned devices directly from the network view by right-clicking one or more selected devices, and then clicking **Security and Patch Information**. This dialog lets you view detection, installation, and repair history, and perform patch management tasks.

Using filters to customize item lists

The **Filter** drop-down list lets you create and apply custom display filters to control the items that display in the right-hand frame of the Security and Patch Manager window. Filters can help you streamline a large amount of security and patch content. You can filter content by operating system and severity.

The **Filter** control can be used in conjunction with the **Type** control to display exactly the security and patch content you're interested in.

To create a new display filter

1. In Security and Patch Security Manager, click the **Filter** drop-down list, and then click **Manage filters**.
2. Click **New**.
3. Enter a name for the new filter.
4. If you want to filter content by operating system, click the check box, and then select the operating systems you want to display.
5. If you want to filter by the severity of the definition, click the check box, and then select the severities you want to display.
6. Click **OK**.

To apply a filter to a content group's display

1. Click the content group in the left-hand pane of the Security and Patch Manager window.
2. Click the **Filter** drop-down list, and then select a filter from the list.

Purging unused definitions

You can purge unused definitions from the Security and Patch Manager window (and the core database) if you determine that it isn't relevant to your environment or if a successful remediation makes the information obsolete.

When you purge definitions, associated detection rule information is also removed from the Detection Rules groups in the tree view. However, the actual associated patch files aren't removed by this process. Patch files must be removed manually from the local repository, which is typically on the core server.

To purge unused definitions

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Purge unused definitions** toolbar button.
3. Select the platforms whose definitions you want to remove. You can select one or more platforms in the list.

If a definition is associated with more than one platform, you must select all of its associated platforms in order for the definition to be removed.

4. Select the languages whose definition you want to remove (associated with the platform selected above).

If you select a Windows or Macintosh platform above, you should specify the languages whose definition you want to remove. If you select a UNIX or Linux platform above, you must specify the Language neutral option in order to remove their language independent definitions.

5. Click **Remove**.

Creating custom definitions and detection rules

In addition to the known vulnerabilities that you update via the LANDesk Security and Patch Manager service, you can also create your own custom (or user-defined) definitions—complete with custom detection rules, associated patch files, and special additional commands to ensure successful remediation.

Vulnerability definitions consist of a unique ID, title, publish date, language, and other identifying information, as well as the detection rules that tell the security scanner what to look for on target devices. Detection rules define the specific platform, application, file, or registry conditions that the security scanner checks for in order to detect a vulnerability (or practically ANY system condition or status) on scanned devices.

Security and Patch Manager's custom vulnerability definitions is a powerful, flexible feature that lets you implement an additional, proprietary level of patch security on your LANDesk system. In addition to enhancing patch security, custom vulnerabilities can be used to assess system configurations, check for specific file and registry settings, and deploy application updates, among other innovative uses that take advantage of the scanning capabilities of the vulnerability scanner.

Creating custom blocked application definitions

You can also create your own custom definitions for the blocked application type. From the **Type** drop-down list, select **Blocked Applications**, enter an executable filename and a descriptive title for the definition, and then click **OK**.

Custom definitions don't necessarily have to perform remediation actions (deploying and installing patch files). If the custom definition is defined with a Detect Only detection rule or rules that can only be detected by Security and Patch Manager, the security scanner looks at target devices and simply reports back the devices where the rule's prescribed condition (i.e., vulnerability) is found. For example, you can write a custom Detect Only rule for the security scanner to check managed devices for the following:

- Application existence
- File existence
- File version
- File location
- File date
- Registry setting
- And more...

You can create as many custom vulnerability definitions as you need to establish and maintain the optimal level of patch security for your environment.

Creating custom definitions

To create custom definitions

1. Click **Tools | Security | Security and Patch Manager**.
2. From the **Type** drop-down list, select **All Types** or **Custom Definitions**. (The **Create custom definition** toolbar button is available only with one of these two types selected, or with the **Blocked Applications** type selected, if you want to create a custom blocked application definition.)

3. Click the **Create custom definition** toolbar button. An editable version of the properties dialog opens, allowing you to configure vulnerability settings.
4. Enter a unique ID for the vulnerability. (The system-generated ID code can be edited.)
5. The type is a Custom Definition and can't be modified.
6. The publish date is today's date and can't be modified.
7. Enter a descriptive title for the vulnerability. This title displays in vulnerability lists.
8. Specify the severity level. Available options include: Unknown, Service Pack, Critical, High, Medium, Low, and Not Applicable.
9. Specify the status for the vulnerability. Available options include: Don't Scan, Scan, and Unassigned. When you specify a status, the vulnerability is placed in the corresponding group in the Security and Patch Manager tree view (see Security and Patch Manager view earlier in this chapter).
10. The language setting for user-defined vulnerabilities is automatically set to INTL (International or Language neutral), which means the vulnerability can be applied to any language version of operating systems and/or applications.
11. The Detection Rules list displays all the rules used by this vulnerability. If you are creating a new custom vulnerability, you should configure at least one detection rule that is used by the security scanner to scan devices for the vulnerability. To add detection rules, click **Add**. (See the procedure below for step-by-step instructions.)
12. If you want to provide additional information about this vulnerability, click the **Description** tab and type your comments in the text box and/or enter a valid Web address where more information is posted.

As with known vendor vulnerabilities, custom vulnerabilities should include one or more detection rules that tell the security scanner what conditions to look for when scanning managed devices. Follow the steps below to create a detection rule for a custom vulnerability.

Creating custom detection rules

To create custom detection rules

1. Right-click a custom definition, and then click **Properties**. (Or double-click the vulnerability definition.)
2. Click the **Add** button located under the Detection Rules list. An editable version of the Rules Properties dialog opens at the dialog's General Information page, allowing you to configure a detection rule.
3. At the General Information page, enter a unique name for the rule. The rule's status cannot be modified here. To change the status of a detection rule, right-click the rule in any list view, and then click **Enable** or **Disable**, depending on the current state. The rule's definition information cannot be modified here either. However, you can enter any information you want in the Comments box.
4. Use the various pages of the Rules Properties dialog to define the detection rule, as described in the rest of this procedure.
5. Open the Detection Logic pages.
6. At the Affected Platforms page, select the platforms you want the security scanner to run on to check for this detection rule's definition. The list of available platforms is determined by the vulnerabilities you've updated via the LANDesk Security and Patch Manager service. Click **Load default platform list** to add the available platforms to the list. You must select at least one platform.

7. At the Affected Products page, associate the rule with one or more specific software applications. First, click **Edit** to open the Selected Affected Products dialog where you can add and remove products in the Affected Products list (this list can be shortened if you like, by clicking the check box at the bottom of the dialog). The list of available products is determined by the content you've updated via the LANDesk Security and Patch Manager service. You do not need to have a product associated with a detection rule. Associated products act as a filter during the security scan process. If the specified associated product is found on the device, the scan quits. However, if the product is found, or if no products are specified, the scan continues to the files check.
8. At the Files page, configure specific file conditions that you want the rule to scan for. Click **Add** to make the fields on this page editable. The first step in configuring a file condition is to specify the verification method. The fields on this tab depend on the verification method you select. To save a file condition, click **Update**. You can add as many file conditions as you like. For a detailed description of this option, see Detection Rule: Files page later in this chapter.
9. At the Registry Settings page, configure specific registry conditions that you want the rule to scan for. Click **Add** to make the fields editable. To save a registry condition, click **Update**. You can add as many registry conditions as you like. For a detailed description of this option, see Detection Rule: Registry tab later in this chapter.
10. At the Custom Script page, you can create a custom VB script to assist with detection for this detection rule. The security scanner agent's runtime properties that can be accessed with a custom script to report its results are: Detected, Reason, Expected, and Found.
11. At the Patch Information page, specify whether the vulnerability associated with this detection rule can be repaired or can only be detected on your managed devices. If you select the repair option, the Patch Download Information and Repair Information fields become editable.
12. If you can repair by deploying a patch, enter the URL to that patch file and specify whether it can be downloaded automatically.

You can attempt to download the associated patch file at this time by clicking **Download**, or you can download it at another time.

13. Also, if you can repair by deploying a patch, enter a unique filename for the patch file and specify whether the patch requires a reboot in order to complete remediation and if the patch requires user input during remediation.

For a detection rule that includes remediation, we strongly recommend you create a hash for the patch file by clicking **Generate MD5 Hash**. The actual patch file must be downloaded before you can create a hash. For more information on the hash, see Detection Rule: Patch Information page.

14. For a rule that allows remediation of the associated vulnerability, you can configure additional commands that are run during the remediation process on affected devices. To configure additional remediation commands, click the Patch Install Commands page, and then click **Add** to select a command type and to make the command's argument fields editable. Additional patch install commands are NOT required. If you don't configure special commands, the patch file executes as it normally would by itself. For a detailed description of this option, see Detection Rule: Patch Install Commands page later in this chapter.

Now that you've created a custom vulnerability definition, you can do the same things with it as you would with a known vulnerability from an industry source. You can set the vulnerability's status to Scan or place it in the Scan group to be included in the next security scan, place it in the Don't Scan or Unassigned group, view affected computers, enable Auto Fix, create a repair job, or clear scan/repair status. To choose an option, right-click a custom vulnerability definition to access its shortcut menu.

Two operations that are unique to user-defined definitions are importing and exporting, and deleting.

Importing and exporting custom definitions

Security and Patch Manager provides a way for you to import and export custom definitions and their detection rules. You can't import and export known industry vulnerability definitions.

Custom definitions are exported and imported as an XML-formatted file.

Import and export is useful if you want to share custom definitions with other core servers. Exporting makes it possible for you to save a backup copy for a definition that you want to remove temporarily from the core database.

You can also use the export/import feature to export a definition, manually edit the exported file as a template and save multiple variations of the definition, and then import the new definitions. If the definition is complex, this procedure can be faster and easier than creating multiple definitions in the console.

To export custom definitions

1. From a Custom Definitions list, select one or more custom definitions.
2. Click the **Export** toolbar button. (Or, right-click the selected definitions, and then click **Export**.)
3. Enter the path to the folder where you want to export the definitions as an individual XML file.
4. If you've exported the definitions before to the specified location and you want to replace it, click the **Overwrite existing definitions**.
5. Click **Export**. Check the Export Status window to see whether the definitions are successfully exported.

An exported definition continues to exist in the core database, and therefore still appears in the Custom Definitions group that corresponds to its status: Unassigned, Scan, or Don't Scan.

6. Click **Close**.

To import custom definitions

1. In the Security and Patch Manager window, click the **Import Custom Definitions** toolbar button.
2. Locate and select one or more definitions (XML file) you want to import, and then click **Open**. If the definition already exists in the core database, you're prompted whether you want to overwrite it. Check the status window to see whether the definition is successfully imported.
3. Click **Close**. Imported definitions (new and updated) are placed in the Custom Definitions Unassigned group.

Deleting custom definitions

If you no longer need a custom definition, you can delete it. Deleting a custom definition removes its information and its associated detection rules from the core database, and from the Security and Patch Manager window. (Exporting does not remove the definition information.)

As with purging known vulnerability information, deleting custom definitions does not remove any downloaded associated patch files. Patch files must be removed manually from the patch repository.

To delete custom definitions, select one or more custom definitions, and then click the **Delete selected custom definitions** button in the toolbar.

Restoring exported custom definitions

If you delete a custom definition that had previously been exported as an XML file, you can restore that definition by importing it back into Security and Patch Manager.

Downloading patches

In order to deploy security patches to affected devices, the patch executable file **MUST** first be downloaded to a local patch repository on your network. The default location for patch file downloads is the core server's /LDLogon/Patches directory. You can change this location on the Patch Location tab of the Download updates dialog.

Patch download location and proxy server settings

Patch downloads always use the download location settings currently found on the Patch Location tab of the Download updates dialog. Also note that if your network uses a proxy server for Internet access, you must first configure the proxy server's settings on the Proxy Settings tab before you can download patch files.

Security and Patch Manager first attempts to download a patch file from the URL (shown on the Patch Properties dialog). If a connection can't be made, or if the patch is unavailable for some reason, then the patch is downloaded from the LANDesk security service, which is a LANDesk-hosted database containing patches from trusted industry sources.

You can download one patch at a time, or a set of patches together at the same time.

To download patches

1. From any Detection Rules group, right-click a detection rule, and then click **Download Patch**. You can also download patches for custom definitions from the detection rule dialog when creating or editing a custom definition.
2. Or, to download a set of patches, select any number of rules in any Detection Rules group, right-click the selection, and then click **Download Patch**.
3. The download operation and status displays in the Downloading Patches dialog. You can click **Cancel** at any time to stop the entire download process.
4. When the download is finished, click the **Close** button.

For more information on patch file download status, see Understanding the Security and Patch Manager window earlier in this chapter.

Uninstalling patches

You can uninstall patches that have been deployed to managed devices.

For example, you may want to uninstall a patch that has caused an unexpected conflict with an existing configuration.. By uninstalling the patch, you can restore the device to its original state.

To uninstall a patch

1. From any detection rule listing, right-click one or more rules, and then click **Uninstall Patch**.
2. Enter a name for the uninstall task.
3. Specify whether the uninstall is a scheduled task or a policy-based scan, or both.
4. If you selected scheduled task, specify which devices from which you want to uninstall the patch.
5. If the patch can't be uninstalled without accessing its original executable file (i.e., to use command-line parameters), and you want to deploy the executable using Targeted Multicast, check the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. See About the Multicast Options dialog below for details.
6. If you selected policy, and you want to create a new query based on this uninstall task that can be used later, click the **Add a query** check box.
7. Select a scan and repair setting from the available list (or create a custom setting for this scan), to determine how the scanner operates on end user devices.
8. Click **OK**. For a scheduled task, you can now add target devices and configure the scheduling options in the Scheduled tasks tool. For a policy, the new policy appears in the Application Policy Management window with the task name specified above. From there you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Removing patches from the core database

To remove patch files permanently, you must delete them from the patch repository, which is typically on the core server.

This chapter provides information on scanning managed devices for a variety of security risks (such as OS and application vulnerabilities, software updates, spyware, system configuration exposures, etc.), remediating affected devices, as well as generating security alerts, logging, and reports.

For information on updating and viewing security content, creating and using custom definitions, and downloading and working with patches, see Managing security content and patches.

Read this chapter to learn about:

Scanning devices

- Scanning devices
- How Security and Patch Manager scans for different content types
- Creating security scan tasks
- Configuring scan options with scan and repair settings
- Viewing detected security data

Remediating devices

- Remediating devices
- How Security and Patch Manager remediates different content types
- Remediation methods
 - Using a scheduled repair task
 - Using a repair policy
 - Using an autofix repair
- What happens on a device during remediation
- Viewing security and patch information for scanned devices

Other security management tasks

- Creating a scheduled reboot task
- Using security alerts
- Using security reports

Scanning devices (for each security content type)

In previous versions, security scanning meant checking the currently installed versions of operating system and application specific files and registry keys on a device against the most current known vulnerabilities in order to identify and resolve security risks in your systems. Now, LANDesk Security services offers expanded security and patch content, enabling you to scan for and remediate even more of today's prevalent security risks.

Depending on your Security Suite content subscription, you can scan for:

- Known vulnerabilities (for Windows, Mac, Linux, and UNIX)
- Custom vulnerabilities (defined by LANDesk Administrator)
- Spyware
- Security threats (local system or platform configuration errors; includes firewall detection and configuration)
- Blocked applications
- LANDesk software updates
- Driver updates
- Software updates
- Antivirus updates (checks for third-party antivirus engines and current pattern files)

Security Suite content subscriptions

For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

How Security and Patch Manager scans for different content types

The table below describes how the security scanner works for each content type:

When scanning for...	Security and Patch Manager scans by...
LANDesk software updates	Using software update definitions published by LANDesk to check for LANDesk software versions.
Windows vulnerabilities	Using vulnerability definitions published by LANDesk (based on official vendor security bulletins) to check for known operating system and/or application vulnerabilities.
Macintosh vulnerabilities	Using vulnerability definitions published by LANDesk (based on official security bulletins) to check for known vulnerabilities.
Linux/UNIX vulnerabilities	Using vulnerability definitions published by LANDesk (based on official security bulletins) to check for known vulnerabilities.
Custom definitions	Using custom vulnerability definitions created by a LANDesk Administrators to check for a user-defined platform, application, file, or registry setting conditions.
Windows security threats	Using definitions published by LANDesk to check for local Windows system configuration errors and exposures.
Spyware	Using spyware detection definitions that check for instances of spyware on scanned devices.

Driver updates	Using third-party driver update definitions that check for driver versions.
Software updates	Using third-party software update definitions that check for software versions.
Antivirus updates	Using antivirus detection definitions that check for instances of antivirus scanner engines and antivirus pattern file versions.
Blocked applications	Uses application definitions published by LANDesk (or user-defined custom blocked application definitions) to immediately deny end user access to the application by editing the local registry. Remediation is NOT a separate procedure. (See the legal disclaimer for the blocked application type.)

To understand how Security and Patch Manager remediates these different content types, see the How Security and Patch Manager remediates different content types table.

Configuring the content of a security scan

After reviewing downloaded definitions and deciding which items you want to scan for, you can perform customized security assessment on managed devices by moving definitions into their respective Scan groups. When the security scanner runs, it always reads the contents of the Scan group and scans for those specific definitions (**Important:** if that type is selected in the task's scan and repair settings). Before scanning devices, you should always make sure the appropriate definitions are in the Scan group. You can move definitions into and out of the Scan group manually at any time.

You can also update security and patch content which, by default, automatically adds new definitions into the Scan group.

Blocked applications are placed in the Unassigned group by default

Keep in mind that the blocked application type is handled differently than the other types. By default, blocked application definitions are placed in the Unassigned group, not in the Scan group.

Security scans add security and patch information to a device's inventory in the core database. This information can be used to generate specific queries, policies, and reports. To view this information, right-click the device and then click **Security and Patch Information**.

Caution about moving definitions from the Scan group

When you move definitions from the Scan to the Don't Scan group, the current definition assessment information (information located in the core database about which scanned devices detected those definitions) is removed from the core database and is no longer available in either the definition Properties dialogs or in the device Security and Patch Information dialogs. To restore that information, you would have to move the definitions back into the Scan group and run the scan again.

Creating security scan tasks

The security and patch scanner can be run directly at a device (Click **Start | All Programs | LANDesk Management | Security and Patch Scanner**), or it can be run as a scheduled task or a policy from the core server.

Scheduled task remediation can be thought of as a push distribution because the patch is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

To create a security scan task

1. Click **Tools | Security | Security and Patch Manager**.
2. Make sure security and patch content has been updated recently.
3. Make sure the Scan group contains only those definitions you want to scan for.
4. Click the **Create a task** toolbar button, and then click **Security scan**. The Create security scan task dialog displays.
5. Enter a name for the scan.
6. Specify whether the scan is a scheduled task or a policy-based scan, or both.
7. Select a scan and repair setting from the available list (or create a custom setting for this scan), to determine how the scanner operates on end user devices.
8. Specify the purpose of the scan by clicking the desired security content types.
9. Click **OK**. For a scheduled task scan, you can now add target devices and configure the scheduling options in the Scheduled tasks tool.

Security scan log file

The security and patch scanner writes a log file for the most recent scan on the device called **vulscan.log**, and also saves the last five log files in chronological order by number. These log files record useful information about the time of the scan, language, platform, and the processes run by the scan.

Viewing the most recent security scan date

To see when the last security scan was run on a device, right-click the device, click **Inventory**, and then scroll down to the **Last Scan Dates** in the right-hand pane of the Inventory view.

Configuring scan options with scan and repair settings

Security and Patch Manager gives you complete control over what the end user sees, device reboot behavior, and the level of interaction the end user is allowed when the security and patch scanner runs on devices. Depending on the purpose or scheduled time of a scan, you may want to show the end user scanner progress and give them the opportunity to cancel or defer an assessment scan or patch deployment remediation.

Scan and repair settings is also where you determine the content of a security scan, by selecting specific definition types.

You do this by creating and applying scan and repair settings (a saved set of configured options) to scan tasks. You can create as many scan and repair settings as you like. Some scan and repair settings might be well suited for a variety of scanning or remediation tasks, while others might be specifically designed for a single task.

To create scan and repair settings

1. In the Security and Patch Manager window, click the **Configure scan and repair settings** toolbar button.
2. Click **New**. Or, you can click **Edit** or **Configure** on any of the task dialogs that let you apply an scan and repair setting.

3. Enter a name for the scan and repair setting
4. Specify the settings on the tabs as desired for the particular task (scan, repair, reboot). For more information about an option, click **Help**.

Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks.

Viewing detected security data

If the security scanner discovers any of the selected definitions, this information is reported to the core server. You can use any of the following methods to view detected security data after running a scan:

By the Detected group

Select the **Detected** group in the Security and Patch Manager window to view a complete listing of all definitions detected by the most recent scan. The Scanned column indicates how many devices were scanned for a definition, and the Detected column shows how many of those devices are affected by that definition.

By a definition

Right-click a definition, and then click **Affected computers** to view a list of devices on which the definition was detected by the most recent scan.

By an individual device

Right-click a specific device in the network view, and then click **Security and Patch Information** to view detailed security assessment information and patch deployment status for the device. For more information, see About the Security and Patch Information dialog.

By a group of selected devices

Select multiple devices in the network view, right-click the group, and then click **Security and Patch Information** to view a list of definitions discovered on one or more of those devices. When you select a definition in the list, the devices on which the definition was detected by the most recent scan display in the bottom pane.

Remediating devices

Once you've updated security and patch content for the content types you've have a license or subscription for, scanned devices, determined which detected security exposures require attention, and downloaded patches, the next step in implementing security and patch management is to remediate (or repair) the security problem.

Remediation solutions and actions are different depending on the type of security risk. Furthermore, some remediation can be done remotely with the Security and Patch Manager tool, while other remediation tasks must be done manually. For example, vulnerabilities are remediated by deploying and installing the necessary security patches on affected devices, while spyware is remediated by removing the infecting spyware itself, and a system configuration security threat is typically remediated by editing the registry or changing some other platform-specific setting. Remediation for each content type is described below:

Known vulnerabilities

For **known vulnerabilities**, remediation entails deploying and installing the appropriate security patch. Windows and Macintosh vulnerability remediation can be performed via the console, as a scheduled task, or policy-based remediation, or as an autofix scan. However, Linux and UNIX vulnerability remediation must be done manually.

Custom definitions

For **custom definitions**, remediation can consist of deploying a custom patch or script that addresses the exposure. Like known vulnerability remediation, these repair tasks can be done via the console.

LANDesk software updates

For **LANDesk software updates**, remediation means the proper version upgrade is installed. You can do this via the console.

Security threats

For **Security threats** (which are local Windows system or platform configuration errors), remediation has to be done manually at the affected device.

Firewall detection and configuration

Some of the Windows security threat definitions are specifically designed to detect and configure firewalls on managed devices.

For example: Configure the Windows Firewall (ST000102), and Internet Connection Firewall (ST000015)

The windows firewall security threat properties includes custom variables that let you configure firewall settings. You can use these security threat definitions to scan for your specified settings and return a vulnerability condition if those settings are not matched. You can then use the customized definition in a repair task during remediation scanning in order to turn on or off the firewall as well as change or reconfigure the firewall's settings on the scanned device.

Windows GPO could change firewall settings

You should be aware that it is possible for a Windows Group Policy Object (GPO) to interfere with firewall settings configured with the security scanner. For example, the firewall settings you define in the Configure the Windows Firewall security threat's custom variables dialog and that are then implemented by a security scanner repair task could be changed back to their original value according to how the settings are defined in an active Group Policy Object.

Spyware

For **spyware**, remediation consists of removing the violating spyware application. This can be done remotely from the console with a repair task.

Real-time spyware detection

You can now also configure a device for real-time spyware monitoring (scanning, detection, and removal). In order to use real-time spyware monitoring, you must enable the settings in the device's agent configuration. On the Agent configuration dialog's Spyware/Application blocker page, check the appropriate spyware monitoring checkboxes.

Important: In order for real-time spyware scanning and detection to work, you must manually enable the autofix feature for any downloaded spyware definitions you want included in a security scan. Downloaded spyware definitions don't have autofix turned on by default.

Blocked applications

For **blocked applications**, remediation is NOT a separate task. Application blocking takes place as part of the security scan itself, by editing the registry on the local hard drive to disable user access to those unauthorized applications. Security and Patch Manager uses the LANDesk Software license monitoring tool's softmon.exe feature to deny access to specified application executables.

Antivirus updates

Antivirus updates detect third-party antivirus scanner engines and antivirus pattern files. When you do a security scan with antivirus update definitions, the scanner checks for the specified antivirus scanner on managed devices and lets you enable/disable certain options such as real-time antivirus scanning. You can also scan for current pattern files and report a device as being vulnerable if the pattern file is out of date.

Remediating Linux and UNIX devices

Linux and UNIX devices must be remediated manually

Supported Windows and Macintosh devices can be remediated remotely from the console, but other platforms such as Linux and UNIX Sun Solaris can only be scanned, not remediated, from the console. You must manually install the appropriate patches on both Linux and UNIX devices in order to remediate them.

How Security and Patch Manager remediates different content types

The table below describes how Security and Patch Manager remediates the various security content types:

When remediating...	Security and Patch Manager remediates by...
LANDesk software updates	Deploying and installing the appropriate LANDesk software update.
Windows vulnerabilities	Deploying and installing the required patch files (patch files must already be downloaded to the local patch repository).
Macintosh vulnerabilities	Deploying and installing the required patch files
Linux/UNIX vulnerabilities	Remediation is performed manually at the affected device.
Custom definitions	Deploying and installing patch files, if the associated detection rule allows remediation, and if the specified patch files are available.
Windows security threats	Remediation is performed manually at the affected device.
Spyware	Removing the detected spyware instance. See the spyware section for more information on real-time spyware detection and removal.
Driver updates	Deploying and installing the appropriate third-party driver update.
Software updates	Deploying and installing the appropriate third-party software update.
Antivirus updates	You can re-enable real-time antivirus scanning if it's been turned off.
Blocked applications (published and custom)	Remediation is NOT a separate procedure. Application blocking is done during the security scan process. The security scan immediately denies end user access to the application by editing the registry. (See the legal disclaimer for the blocked application type.)

To understand how Security and Patch Manager scans for these different content types, see the How Security and Patch Manager scans for different content types table.

Remediating from the console

As stated above, Windows and Macintosh vulnerabilities, custom definitions, LANDesk software updates, and blocked applications can be remediated from the console. The sections below describe these different methods.

Enhanced patch deployment remediation

Security and Patch Manager does a smart remediation by installing only those patches that are needed on each individual device, not all of the patches referenced by all of the vulnerabilities included in the repair job. The tool also takes advantage of LANDesk's enhanced package deployment capabilities for fast and efficient patch deployment, such as: Targeted Multicast, peer download, and checkpoint restart. For more detailed information about these software distribution features, see *Distributing software and files*.

Remediating one or more definitions at a time

You can remediate a single detected definition or a set of them with any of the three remediation methods described below.

To remediate one definition at a time, right-click the item and then click **Repair**.

To remediate a set of definitions together, copy definitions from any of the content groups into a custom group (see *Understanding the Security and Patch Manager window*), right-click the group, and then click **Repair**. The Auto Fix method isn't available for custom groups; however, you can multi-select definitions in a listing, right-click and select **Auto Fix**.

Remediation methods

Security and Patch Manager provides the following methods to remediate from the console:

- Scheduled task
- Policy-based
- Auto Fix

Scheduled task remediation can be thought of as a push distribution because the patch is pushed from the core server to devices, while a policy is considered a pull distribution because the policy agent on the device checks the core server for applicable policies and then pulls the patch from the core server.

Using a scheduled repair task

Scheduling a remediation or repair task is useful if you want to set up the task to run at a specific time in the future, or as a recurring task. Security and Patch Manager uses the Scheduled Tasks tool to configure and process a scheduled repair task.

Supported platforms for scheduled task remediation

Scheduled task remediation is supported on both Windows and Macintosh devices.

To create a scheduled repair task

1. Click **Tools | Security | Security and Patch Manager**.
2. Right-click a single definition from one of the content groups, or right-click a custom group of definitions, and then click **Repair**. Or, you can click the **Create a task** toolbar button, and then click **Repair**. The Schedule repair dialog displays.
3. Edit the **Task name** if you want to change the name of the repair task.
4. Click the **Repair as a scheduled task** check box.
5. Specify which devices you want to repair. If you want the current affected devices automatically added to the target list in the Scheduled Tasks window, click the **Add all affected devices** check box. The vulnerable devices are those devices where the vulnerability was detected by the last scan. You can also add more targets once the task is created in the Scheduled Tasks window.
6. If you want patches to be deployed using Targeted Multicast, check the **Use multicast** check box. To configure Multicast options, click the **Multicast Options** button. See About the Multicast Options dialog below for details.
7. If you want to use peer download strictly for patch deployment, click the **Download patch only from local peers** check box. If this option is selected, the patch file is only deployed if it currently resides in either the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, it must be in one of these two places.
8. Specify whether to only download the patch and not deploy and install it on affected devices.
9. Select a scan and repair setting for this repair task. The scan and repair setting determines the scanner display, reboot, and user interaction behavior on scanned devices, as well as the actual content that is being scanned.
10. Click **OK**.
11. The task appears in the Scheduled Tasks window with the job name specified above, where you can further customize the target device list and configure scheduling options.

Using a repair policy (Windows only)

Policy-based remediation offers flexibility by letting you dynamically target devices based on the results of a custom LDAP or core database query. For example, you can configure a remediation policy so that it runs only on devices in a particular directory container, or only on devices running a specific OS (or any other inventory attribute that can be queried). Security and Patch Manager uses policies in the Scheduled tasks/Software distribution tool to configure and process remediation policies.

Supported platforms for policy-based remediation

Policy-based remediation is supported on Windows devices only. Macintosh devices can't be remediated via the application policy method.

In order to be remediated by a policy, a device must have the Software distribution agent installed. When the agent runs, it checks the core database for policies that might apply to it. If such policies exist, a dialog appears at the device showing recommended and optional policies (required policies are automatically applied).

Remediation (or repair) policies operate in much the same way as application policies do, except you're distributing patch files instead of application files. Policy management prerequisites, task flow, policy types, and static and dynamic targeting are essentially identical between repair policies and application policies. For more information on policies, see the software distribution chapter.

To create a policy-based remediation

1. Click **Tools | Security | Security and Patch Manager**.
2. Right-click a single definition from one of the content groups, or right-click a custom group of definitions, and then click **Repair**. Or, you can click the **Create a task** toolbar button, and then click **Repair**. The Schedule repair dialog displays.
3. Edit the **Task Name** if you want to change the name of the repair task.
4. Check the **Repair as a Policy** check box.
5. If you want to create a new query, based on this vulnerability definition, that can be used later to scan other managed devices, check the **Add a query** check box.
6. If you want to use peer download strictly for patch deployment, click the **Download patch only from local peers** check box. If this option is selected, the patch file is only deployed if it currently resides in either the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, it must be in one of these two places.
7. Specify whether to only download the patch and not deploy and install it on affected devices.
8. Select a scan and repair setting for this repair policy. The scan and repair setting determines the scanner display, reboot, and user interaction behavior on scanned devices, as well as the actual content that is being scanned.
9. Click **OK**.
10. The new policy appears in the Policies group in the Scheduled Tasks window with the name specified above. From there you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Using an autofix repair

Auto Fix is a convenient, integrated method for quick remediation in cases where you don't want to create a scheduled task or policy-based repair task. For example, if there is a new known vulnerability that you want to scan for and repair in a single process, you can use the Auto Fix feature.

Auto fix is available for the following content types: vulnerabilities, spyware, LANDesk software updates, and custom definitions.

Requirements for using Auto Fix

Only Administrators or users with the Patch Manager right AND the Default All Machines scope can enable the Auto Fix feature for applicable definitions. LANDesk users without either the LANDesk Administrator or Patch Manager right won't even see this option on a definition's shortcut (right-click) menu. For more information on rights and scope, see Role-based administration.

Auto fix has to be enabled in two places in order to work properly. The first setting is on the patch file itself, and the second setting is the scan and repair setting applied to the scheduled scan task. If either one of these two item's autofix option is NOT enabled, autofix will not happen.

When Auto Fix is enabled (in both places mentioned above), the next time the security scanner runs (either manually or via a scan task), Security and Patch Manager automatically deploys and installs the required patch on any affected device. With Auto Fix, if a patch requires a reboot, the target device always automatically reboots.

You can enable Auto Fix for an individual definition, or a multi-selected group of definitions at once.

To configure Auto Fix remediation

1. Click **Tools | Security | Security and Patch Manager**.
2. Right-click one or more selected definitions from one of the content groups. (You can't enable autofix on a custom group.)
3. Click **Autofix when scanning**.
4. Now run the security scanner on the devices you want to scan and automatically remediate using a scheduled security scan task with an scan and repair setting where the autofix option is enabled.

What happens on a device during remediation

Automated remediation entails deploying and installing patches on managed devices, by any of the three methods described in the sections above.

It is important to remember that a repair job can include remediation for one or more detected security definitions. Furthermore, a single detected definition can require the installation of one or more patches to fix. Because of these factors, remediation might imply the installation of just one patch file on the device, or the installation of several patch files on the device, depending on the number and type of detections.

Almost all patch files install silently (or transparently), requiring no user interaction at the end user device itself. Some Windows 9.x patches and non-English patches do not install silently. You can tell whether a patch installs silently or not by checking the Silent Install column in a patch listing. For more information, see Understanding the Security and Patch Manager window earlier in this chapter.

Configuring security scanner display and interaction on end user devices

However, whether a patch file can install silently or not, you can now configure how much you want the security scanner to display and prompt for input on the end user device with the scan and repair setting feature.

Consolidated reboot

If a patch file installation requires a reboot (AND the Never reboot option isn't selected on the Reboot tab of the scan and repair setting applied to the task in question), Security and Patch Manager first installs ALL of the specified task's patches on the device, and then reboots the device once.

Additional commands (for custom definitions only)

Custom definition remediation can include special additional commands that are defined when you create a custom detection rule. Additional commands run in the order specified on that rule's Commands tab, and according to the arguments for each command. Additional commands can run before, during, or after the patch file itself executes.

Viewing security and patch information for scanned devices

As mentioned above, one way to view scanned security data is by device. To do this, right-click a single device or a group of selected devices, and then click **Security and Patch Information**.

This page provides many useful functions. With one or more devices selected, you can:

- View detected definition lists
- View detailed information about when and why the detection occurred
- View installed patch and software update lists
- View detailed information about when the patch was installed or uninstalled
- Clear patch install status
- View repair history data
- Clear repair history data

You can also right-click definitions and detection rules in their respective item lists to run common tasks for one or more affected devices.

Verifying remediation status

After performing remediation on affected devices, Security and Patch Manager reports the status of each patch installation. You can check the status of patch installation per vulnerability/definition and per target device.

To verify patch installation on a device

1. Run the security scanner on the device.
2. Right-click a remediated device in the network view, and then click **Security and Patch Information**.
3. Click the **Installed Patches** object in the left-hand pane.
4. Check the **Patch Information** fields at the bottom of the dialog.

The **Install status** field indicates whether the installation was successful. Possible states include: Succeeded, Failed, and Failed to Download.

Clearing vulnerability scan and repair status by vulnerability

If a patch installation failed, you must first clear the install status information before attempting to install the patch again. You can clear the install (repair) status for the selected device by clicking **Clear** on this dialog. You can also clear the patch install status by vulnerability.

You can clear vulnerability scan and repair status information for all devices affected by a vulnerability (or vulnerabilities) with the **Clear scan/repair status dialog**. As stated above, if a patch installation fails, you must first clear the install (repair) status before attempting to install the patch again.

You can also use this dialog to remove vulnerability scan information from the database for one or more vulnerabilities.

To clear vulnerability scan and repair status, right-click the vulnerability and select **Clear scan/repair status**, select the desired options, and then click **Clear**.

Other security management tasks

Creating a scheduled reboot task

Security and Patch Manager provides a tool that lets you create a device reboot task. A reboot task can be useful when you want to install patches (without rebooting) as a single process and then reboot those remediated devices as another separate task. For example, you can run a scan or a patch install task during the day, and then deploy a reboot only task at a more convenient time for end users.

To create a reboot task

1. Click **Tools | Security | Security and Patch Manager**.
2. Click the **Create a task** toolbar button, and then click **Reboot**.
3. Specify whether the reboot is a scheduled task or a policy-based scan, or both.
4. Select a scan and repair setting from the available list (or create a custom setting for this scan), to determine how the scanner operates on end user devices.

Note: Only the reboot settings in the scan and repair setting are used by a reboot task.

5. Click **OK**. For a scheduled task, you can now add target devices and configure the scheduling options in the Scheduled tasks tool. For a policy, the new policy appears in the Application Policy Management window with the task name specified above, where you can add static targets (users or devices) and dynamic targets (query results), and configure the policy's type and frequency.

Using security alerts

You can configure vulnerability alerting so that you can be notified when specific vulnerabilities are detected on managed devices in your system. Security and Patch Manager's vulnerability alerting uses the standard LANDesk alerting tool.

A vulnerability must be copied to the Alert group in order to generate an alert when detected. A vulnerability in the Alert group is a copy, and also resides in the Scan group. After placing the desired vulnerability definitions in the Alert group (either manually, or by specifying the severity level vulnerabilities to automatically be placed during downloads), you can configure the alert interval in the Configure alerts dialog.

To configure vulnerability alerting

1. Specify which vulnerabilities will generate an alert by manually placing already downloaded vulnerability definitions into the Alert group.
2. Or click the **Configure alerts** toolbar button to open the Configure alerts dialog, and then select the definitions (by severity level) you want to be automatically placed in the Alert group during a download process. You can select more than one vulnerability severity level. These vulnerability definitions will also automatically be placed in the Scan group. (For more information on the severity levels, see About the Configure alerts dialog.)
3. At the Configure alerts dialog, specify a minimum alert interval for alerting.

Using security reports

Security and Patch Manager is represented by several security-related reports in the Reports tool. These reports provide a variety of useful definition assessment, patch deployment, and remediation status information for managed devices on your network, for all of the content types.

In order to access the Reports tool, and generate and view reports, a LANDesk user must have either the LANDesk Administrator right (implying full rights) or the specific Reports right.

Security and Patch Manager reports follow the same rules as reports in the Software License Monitoring group, including their ability to be copied, removed, exported, and so on from the My Reports and User Reports groups.

Running and publishing reports

You can run any report from the Reports window. From the Reports window, right-click the report you want to run, and then click **Run** (or, click the **Run** toolbar button). The report data displays in the Report View.

You can also publish reports to a secure file share where they can viewed by any user you've given the proper access credentials.

For more information about using the Reports tool, and a complete listing of the Security and Patch Manager reports (with descriptions), see Managing Reports.

Using LANDesk trusted access

LANDesk Trusted Access is the latest offering in LANDesk Security Suite's comprehensive security management solution. LANDesk Trusted Access allows you to protect your network from unauthorized access and external security threats such as vulnerable devices or malicious intrusions that can infect and damage your network.

Trusted access lets you define custom security policies, scan managed and unmanaged devices for policy compliance, verify the health status (or posture) of connecting devices, and deny or allow access to your critical network resources based on the device's compliance to your security policy. Healthy (or trusted) devices are granted full network access. However, if a device is determined to be unhealthy, it is blocked from accessing the network and remains in a virtual quarantine area where it can either be repaired with the LANDesk Security and Patch Manager remediation capabilities or be allowed limited network access.

LANDesk's two trusted access solutions

LANDesk Trusted Access enforces endpoint perimeter security by using industry standard security technologies and systems. LANDesk offers two solutions to implement trusted access services:

- **Proprietary LANDesk DHCP solution**
- **Integrated Cisco NAC solution**

This guide provides detailed information on how to set up, configure, enable, and use both of these solutions.

This introductory chapter gives a basic overview of trusted access technology and services; describes relevant Security Suite prerequisites and tools; compares the two LANDesk Trusted Access solutions; and includes links to the relevant sections on setting up and using each solution.

Important: Technical knowledge and expertise required for setting up LANDesk Trusted Access

This guide adequately describes all the concepts and procedures necessary to install, configure, and use LANDesk Trusted Access services for both the LANDesk DHCP and Cisco NAC solutions.

Note that LANDesk Trusted Access requires additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with either Cisco Network Access Control (NAC) and Cisco Secure Access Control Server (ACS) configuration and operation, and/or DHCP server management and DHCP protocols, as well as advanced networking infrastructure design principles and administration.

You should recognize that in order to set up LANDesk Trusted Access you may need to consult with LANDesk technical support representatives and/or affiliated LANDesk system engineers. However, you can be confident that once configured and implemented properly, LANDesk Trusted Access will significantly increase the overall security and protection of your corporate network.

Read this chapter to learn about:

LANDesk Trusted Access overview

- LANDesk Trusted Access services overview
 - Compliance security policies
 - Understanding the basic trusted access components
 - Security Suite prerequisites
 - Supported device platforms for compliance scanning
 - Role-based administration with LANDesk Trusted Access
- Understanding the two solutions and selecting LANDesk DHCP or Cisco NAC
 - Using the LANDesk DHCP solution (links to a separate chapter)
 - Quickstart task list for setting up a LANDesk DHCP implementation
 - Using the Cisco NAC solution (links to a separate chapter)
 - Quickstart task list for setting up a Cisco NAC implementation

LANDesk Trusted Access overview

LANDesk Trusted Access adds an extra layer of protection to your network by letting you prevent vulnerable or corrupted devices from gaining network access, as well as protect critical network resources from connected system that become corrupted.

LANDesk Trusted Access provides flexibility in implementing network access control functionality on your network by supporting common industry standards and methodologies, such as the Cisco NAC initiative, and by offering its own DHCP standards based solution. With network access control, you can evaluate the security credentials of any device as soon as it attempts to connect to your network (by comparing it to custom security policies), monitor the security state of devices that are already connected, allow or deny network access, quarantine devices that fail to meet the security policy requirements, and remediate vulnerable devices so they can be rescanned for security policy compliance and allowed network access once they are deemed healthy.

Compliance security policies

Compliance security policies are comprised of rules that verify the health state of a device by checking for: vulnerabilities (in the form of missing or obsolete OS and application patches), software updates, antivirus engine and signature files, firewall presence and settings, and spyware. For more information on defining a compliance security policy in the Security and Patch Manager tool in the console, see [Configuring compliance security and publishing trusted access settings](#).

The sections below describe the basic components of a LANDesk trusted access implementation and the role of each component and how they interact. More detailed diagrams and process flows are shown in the topic covering each specific solution, respectively. For more information, see:

- [Using the LANDesk DHCP solution](#)
- [Using the Cisco NAC solution](#)

Summary of LANDesk Trusted Access benefits and features

With LANDesk Trusted Access, you can:

- Create and enforce customized compliance security policies
- Implement stronger, around-the-clock, enterprise security
- Assess the security credentials (health status) of connecting devices
- Prevent infected or corrupted systems from accessing the network
- Quarantine non-compliant devices in a secure area
- Remediate infected devices to bring them into compliance
- Reduce downtime due to infections from malicious intrusions
- Protect your network, systems, applications, and data from external threats
- Extend existing security technologies and standards

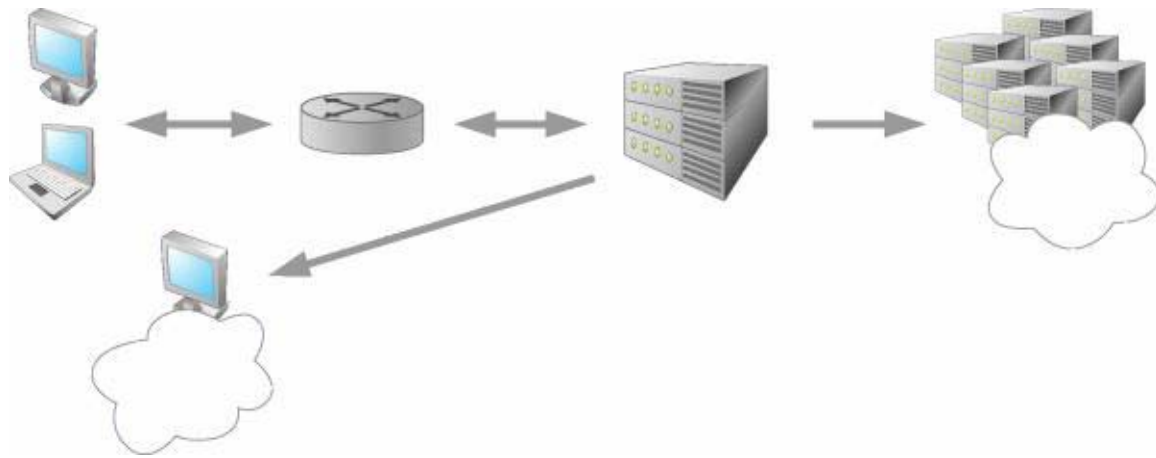
Understanding the basic trusted access components

This section describes the basic components, and the role and interaction of each component, in a LANDesk Trusted Access implementation.

Component	Description
-----------	-------------

Devices attempting to access the network	<p>Includes occasionally connecting or mobile laptops, visiting contractors and guest users, as well as regular network users that attempt to access the corporate network.</p> <p>Devices with a trust agent installed (LANDesk Trust Agent or LTA for LANDesk DHCP trusted access; Cisco Trust Agent or CTA for Cisco NAC trusted access) can communicate with the policy server or posture validation server in order to send and receive health credential information, and can be repaired by the remediation server if vulnerabilities are detected during the security scan.</p> <p>Without a trust agent, a device can't communicate with the posture validation server and can't be remediated. When a device without a trust agent is scanned for the first time, the device should be directed to a Web page with links to install the appropriate trust agent. For more information, see Using the HTML template pages. (Note: The Cisco NAC solution doesn't redirect to a Web page. Instead, the device displays a message box configured by the network administrator (which could specify a web page if the administrator sets it up that way.)</p>
Network access control device	<p>The Cisco router (working in conjunction with the Cisco Secure ACS) in a Cisco NAC environment.</p> <p>The LANDesk DHCP server (configured with "scopes" representing virtual routers with both a quarantine subnet and a primary subnet) in a LANDesk DHCP environment.</p> <p>The network access device functions as the "first hop" network device from the device perspective that begins the posture validation and authentication process.</p>
Policy server	<p>A dedicated back-end server also known as the posture validation server that evaluates the posture credentials (state) of devices requesting access based on the compliance rules (security policy) published to it from the LANDesk core server. Sends a validation response (healthy, unhealthy, etc.) via the network access control device.</p> <p>The posture validation server is used by both the LANDesk DHCP and the Cisco NAC trusted access implementations.</p>
Corporate network	<p>Critical network area and resources that LANDesk trusted access protects from unhealthy, infected, or otherwise vulnerable devices.</p>
Quarantine VLAN	<p>Virtual safe network area where non-compliant devices can be secured and either remediated, rescanned, and then granted full access to the corporate network, or retained with restricted access to network resources such as the Internet.</p>

Basic components and process flow



Devices attempting network access:

(Managed and unmanaged regular user and/or visitor devices)

Quarantine VLAN:

(Safe area to secure and/or remediate non-compliant, unhealthy devices)

Network access control device:

(Router)

Policy server:

(Posture validation server that evaluates and enforces compliance security policy)

Corporate network:

(Network access granted to compliant, healthy devices)

Security Suite prerequisites

In order to use the LANDesk Trusted Access feature, you must have a valid Security Suite license (core server activation). Trusted access requires not only the scanning and remediation capabilities of the Security and Patch Manager tool, but Security Suite content subscriptions in order to download the vulnerability, spyware, system configuration threat, and virus definitions that are used to create custom compliance criteria and rules or security policies.

A new group named Compliance has been added to the Security and Patch Manager's tree view. Users with the Security and Patch Compliance right can add and remove security type definitions into and from the Compliance group. Security definitions contained in the Compliance group comprise the compliance security policy, and are scanned for on connecting devices in order to determine their health status.

For more information on Security Suite content subscriptions, see Using Security and Patch Manager.

Supported device platforms for compliance scanning

As with its underlying Security and Patch Manager tool, LANDesk trusted access services supports most of the standard LANDesk Management Suite device platforms, including the following operating systems:

- Windows NT (4.0 SP6a and higher)
- Windows 2000 SP4 / 2003 / XP SP1

For information on configuring managed devices for compliance scanning (installing the appropriate trust agent to allow communication with routing devices and posture validation servers), see the appropriate section for LANDesk DHCP and Cisco NAC:

- Installing the LANDesk Trust Agent on devices to enable compliance scanning
- Installing the Cisco Trust Agent on devices to enable compliance scanning

Role-based administration with LANDesk trusted access

LANDesk Trusted Access relies on the following two Security and Patch Manager rights and the LANDesk Administrator right.

Security and Patch Manager right

This right is required to see and access the Security and Patch Manager tool, and download security content updates need to define compliance rules.

Security and Patch Compliance right

This right is required to add or remove security definitions from the Compliance group.

LANDesk Administrator right

This right is required to configure devices with trust agents for compliance scanning, and to configure trusted access services in the console.

Note: The LANDesk Administrator right implies all other rights, including the two security-related rights mentioned above.

Understanding the two solutions and selecting LANDesk DHCP or Cisco NAC

The following section describes the pros and cons for both the LANDesk DHCP solution and the Cisco NAC solution for LANDesk Trusted Access.

Evaluating the LANDesk DHCP solution

Pros:

- Uses DHCP filtering
- No specific hardware requirements
- Less expensive

Cons:

- Less secure
- Windows only trust agent
- Requires dedicated machine for LANDesk DHCP server
- Requires network infrastructure changes

Evaluating the Cisco NAC solution

Pros:

- Strong security
- Includes Cisco support

Cons:

- More expensive (especially if you don't already have Cisco hardware in place)
- Vendor specific hardware
- Windows only trust agent
- Potentially significant network configuration changes
- May not be suitable for small businesses

Choose a LANDesk Trusted Access solution

Click on the links below to learn how to set up, configure, and use each of the LANDesk Trusted Access solutions:

- [Using the LANDesk DHCP solution](#)
- [Quickstart task list for setting up a LANDesk DHCP implementation](#)
- [Using the Cisco NAC solution](#)
- [Quickstart task list for setting up a Cisco NAC implementation](#)

This chapter describes how to plan, set up, configure, and enable the LANDesk DHCP implementation of LANDesk Trusted Access.

With the LANDesk DHCP solution, a DHCP server is used for IP address filtering and routing. The LANDesk DHCP server works in conjunction with your primary DHCP server to assign IP addresses to devices attempting to access the network, and communicates with the posture validation server to verify the health or posture of devices attempting to access the network. (Diagrams below show the components and process workflow of a LANDesk DHCP trusted access implementation.) Essentially, in a LANDesk DHCP implementation, the LANDesk DHCP server acts as the network access device that allows or denies access to the network based on device health credentials.

Also, with the LANDesk DHCP solution, you can add specified devices to an exclusion list (identified by their machine or MAC address) if you want them to bypass the posture validation process altogether and allow them immediate access to your corporate network.

In addition to the specific LANDesk DHCP server component, you must also set up a posture validation server and a remediation server in order to implement LANDesk Trusted Access.

Important: Technical knowledge and expertise required for setting up LANDesk Trusted Access

Note that LANDesk Trusted Access requires additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with either Cisco Network Access Control (NAC) and Cisco Secure Access Control Server (ACS) configuration and operation, and/or DHCP server management and DHCP protocols, as well as advanced networking infrastructure design principles and administration.

Read this chapter to learn about:

Setting up a LANDesk DHCP implementation of trusted access

- Quickstart task list for setting up a LANDesk DHCP implementation
- Understanding the LANDesk DHCP components and process workflow
- Network topology and design considerations for a LANDesk DHCP implementation
- Installing the LANDesk Trust Agent on devices to enable compliance scanning
- Setting up and configuring a posture validation server
- Setting up and configuring a remediation server
- Setting up a LANDesk DHCP server

What you should do after setting up a LANDesk DHCP implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk Trusted Access is to: define your compliance security policy, and publish trusted access settings to posture validation servers and remediation servers. These tasks are the same and apply to both the LANDesk DHCP and the Cisco NAC solutions. For information on performing these tasks, see *Configuring compliance security and publishing trusted access settings*.

Additionally, to learn more about other ongoing trusted access management tasks such as: ensuring trusted access services is enabled (turned on), using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing to posture validation servers and remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see Managing compliance security.

Quickstart task list for setting up a LANDesk DHCP implementation

Use this task checklist to help keep track of the steps required to set up the LANDesk DHCP solution. Use this Quickstart task list for setting up a LANDesk DHCP implementation.

Understanding the LANDesk DHCP components and process workflow

This section describes the components that comprise a LANDesk DHCP solution. Additionally, this section describes what happens when a device attempts to access or connect to the corporate network when LANDesk Trusted Access is enabled. Scenarios with and without a LANDesk Trust Agent (LTA) installed on the device are covered in the diagrams and process workflows below.

The following components are required for the LANDesk DHCP-based trusted access service.

Required components

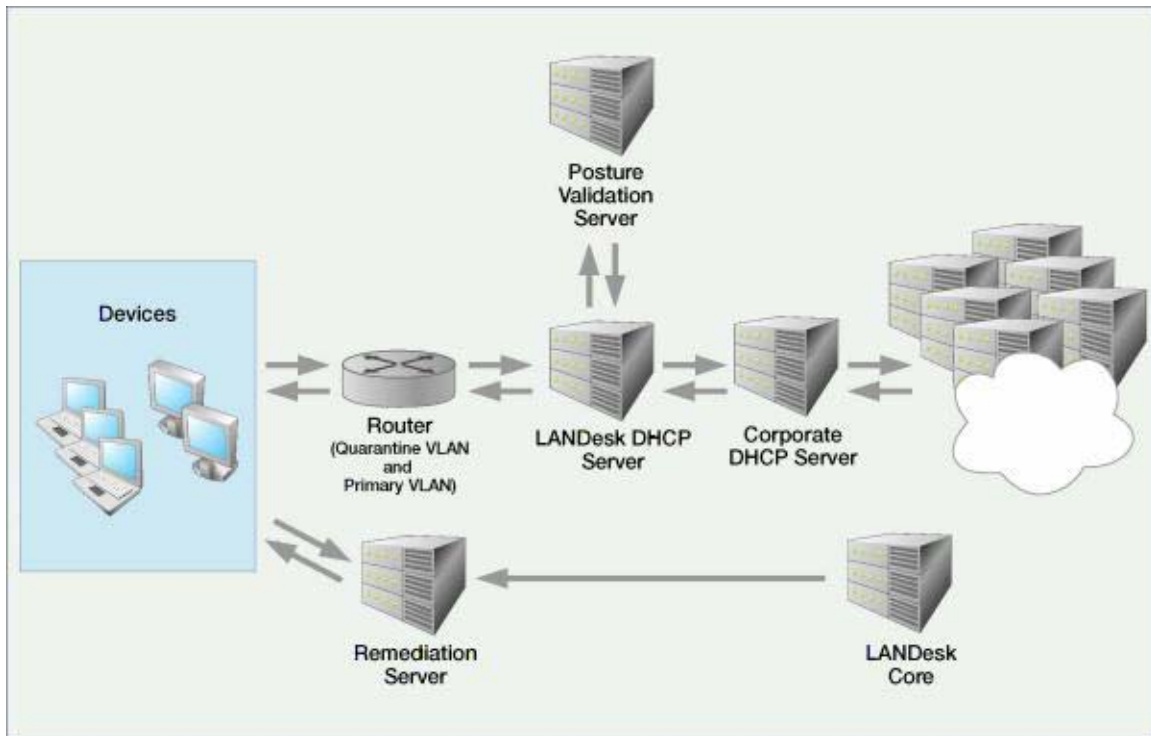
Component	Description
LANDesk core server	Provides the Security and Patch Manager tool used to: download security content (such as OS and application vulnerability definitions, spyware definitions, system configuration security threats, antivirus and firewall configuration definitions, etc.), define compliance criteria, configure posture validation servers and remediation servers, and configure and publish trusted access settings (including compliance security rules or policies and remediation resources for scanning and repairing devices).
Corporate DHCP server	Provides permanent IP addresses to devices whose posture is validated as being healthy. Communicates with the LANDesk DHCP server via a software plug-in installed on the primary DHCP server.
Posture validation server	Determines whether the connecting device has a healthy or unhealthy posture based on two factors: your compliance security policy (the contents of the Compliance group in the Security and Patch Manager tool) AND the number of hours since a healthy scan as specified in the Definition of healthy setting in the Configure trusted access dialog. The posture validation server is the policy decision point in the validation process.
Remediation server	Contains the necessary setup and support files (security client, security type definitions and required patches, as well as the HTML template pages) used to scan devices for vulnerabilities identified by your security policy and remediate (repair) any detected vulnerabilities so that the device can be scanned as healthy or

	compliant and access the network.
LANDesk DHCP server	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the posture validation server to evaluate the posture credentials of the endpoint device. Assigns temporary IP addresses to devices seeking network access, until the device meets compliance security criteria and can be given a permanent IP address from the primary DHCP server. In other words, in a LANDesk DHCP environment, the DHCP server is the policy enforcement point on the network and grants or denies access privileges.
Router	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the LANDesk DHCP server to evaluate the posture credentials of the endpoint device. In a LANDesk DHCP server environment, the router/switch needs to be configured to support BOOTP/DHCP forwarding.
Devices	Mobile or guest user devices, as well as regular network user devices, attempting to access your corporate network. Typical endpoint devices include desktop computers and laptops but may also be "clientless" devices such as printers, etc. LANDesk Trusted Access allows you to evaluate the health status of these connecting devices and control network access based on their posture credentials.

The following diagrams show a typical configuration of the components described above, as well as the posture validation process or workflow between those components.

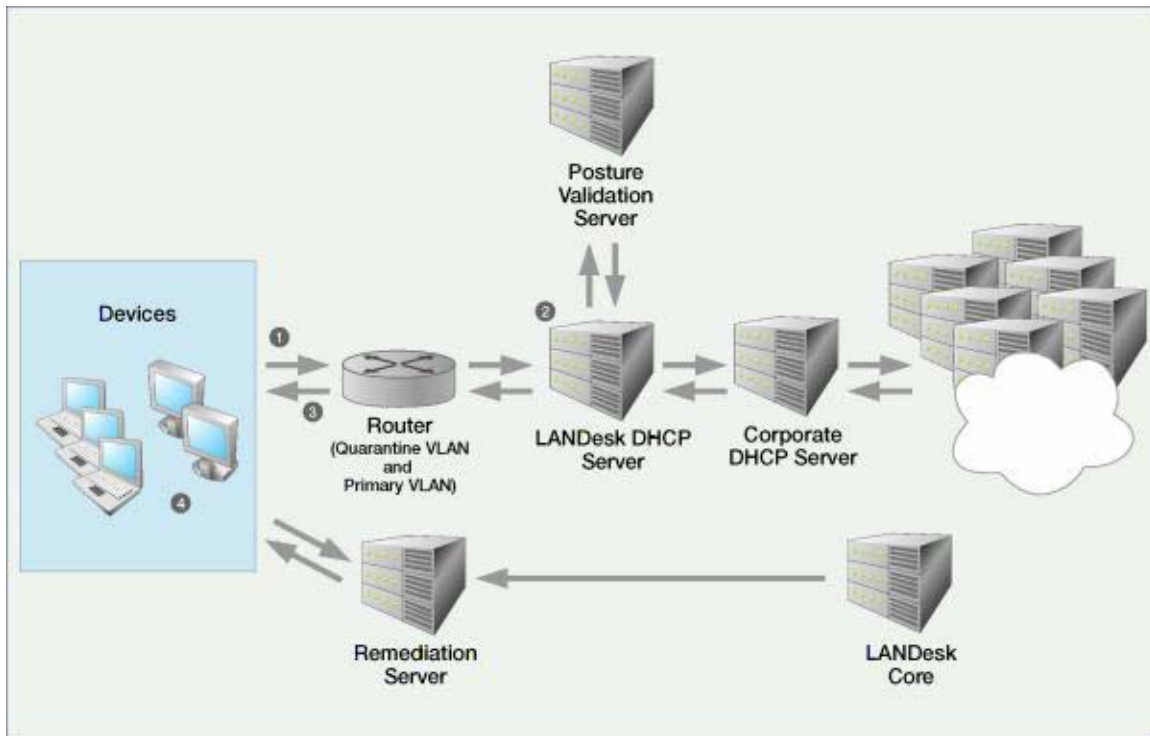
LANDesk DHCP components

The diagram below shows the specific LANDesk DHCP components:



Posture validation process for a device without the LTA installed

The diagram below shows the workflow or communication flow between the various components in a LANDesk DHCP environment when the device attempting to access the network does not have the LANDesk Trust Agent (LTA) installed. The callout numbers represent each stage of the process and are explained in the steplist below.



Process workflow:

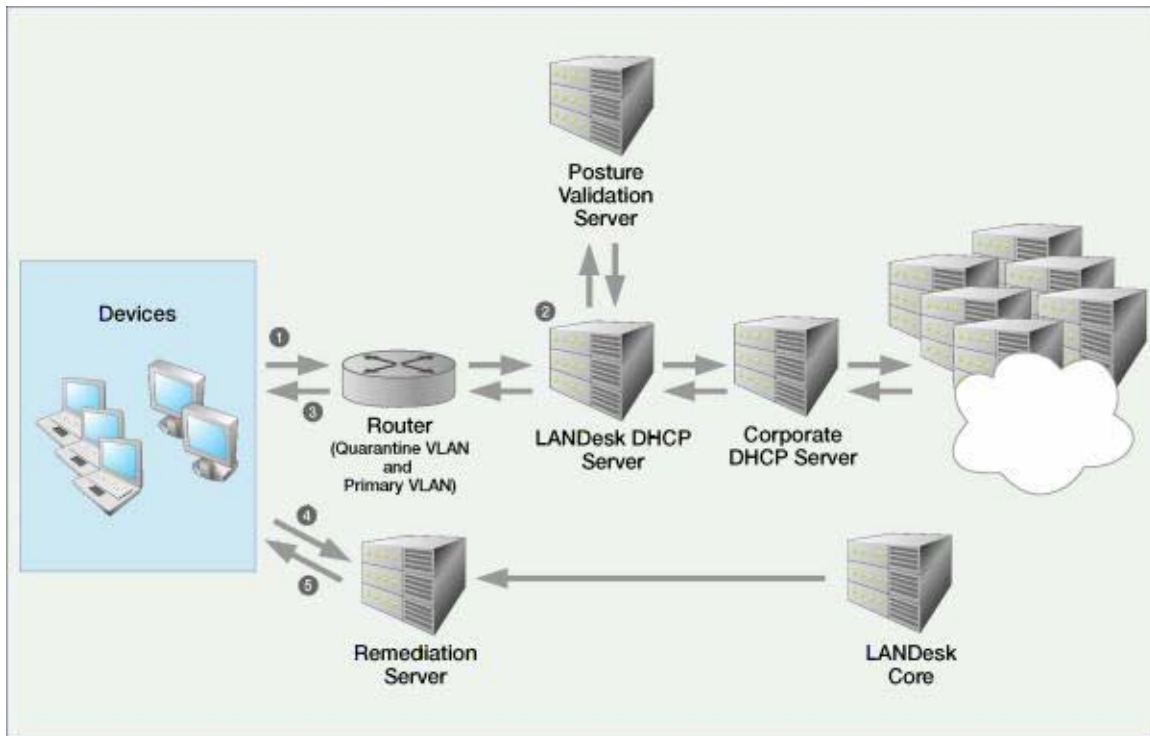
1. A device that is NOT configured with the LANDesk Trust Agent (LTA) makes an initial attempt to access the corporate network via the LANDesk DHCP server and requests an IP address.
2. The LANDesk DHCP server determines if this is a supported platform by looking at Option 60. If it is a supported platform, the LANDesk DHCP server determines whether the health status of the device is known/cached (or if the device is included in the Exception List).
3. The LANDesk DHCP server returns a Quarantine VLAN IP address to the device (from the IP address pool). If the device is not a supported platform, or if it is included in the Exception list, then the request is forwarded to the primary corporate DHCP server.
4. At this point, the device can either install the LANDesk Trust Agent and run the security client (from the HowToInstall HTML page) in order to scan for and remediate any existing vulnerabilities, and become healthy or compliant with the corporate security policy, and granted access to the network. Or, the device can simply remain on the Quarantine VLAN with restricted network access, depending on the access control rules (ACLs) defined on the router by the network administrator.

Posture validation process for a device with the LTA installed

The diagrams below show the workflow or communication flow between the various components in a LANDesk DHCP environment when the device attempting to access the network has the LANDesk Trust Agent (LTA) installed. The callout numbers represent each stage of the process and are explained below.

The LANDesk DHCP posture validation process has been divided into three phases.

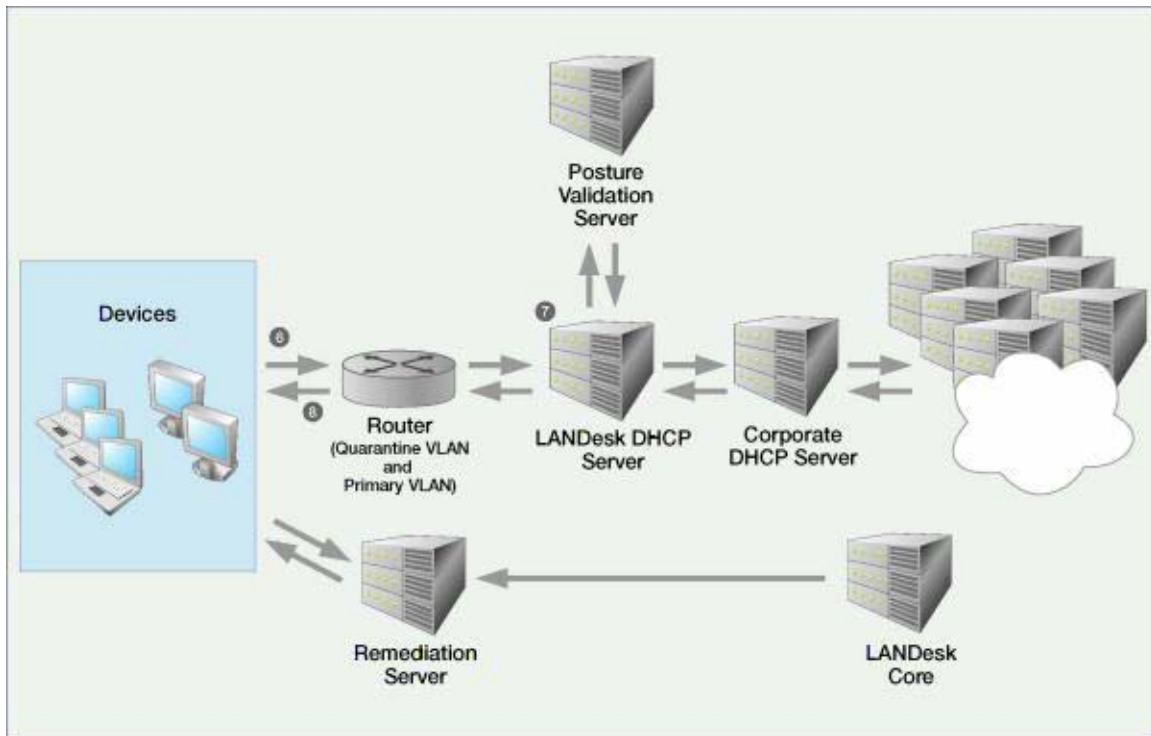
Phase 1: Initial access attempt (temporary/quarantine IP address assigned; remediation offered)



Process workflow for the initial access attempt:

1. A device that is configured with the LANDesk Trust Agent (LTA) makes an initial attempt to access the corporate network via the LANDesk DHCP server and requests an IP address.
2. The LANDesk DHCP server determines if this is a supported platform by looking at Option 60. If it is a supported platform, the LANDesk DHCP server determines whether the health status of the device is known/cached (or if the device is included in the Exception List).
3. The LANDesk DHCP server returns a Quarantine VLAN IP address to the device (from the IP address pool). If the device is not a supported platform, or if it is included in the Exception list, then the request is forwarded to the primary corporate DHCP server.
4. Because the trust agent is installed on the device, its browser can launch and be redirected to the Install page on the remediation server that should have already been published from the core server. This page has links that let you install agents and run the security scanner to scan for compliance and perform necessary remediation.
5. Run the security client (scanner) in order to scan for and remediate any existing vulnerabilities and other security risks defined in your compliance security policy. Successful remediation makes the device compliant or healthy so that it can proceed to the next steps in the LANDesk DHCP posture validation process.

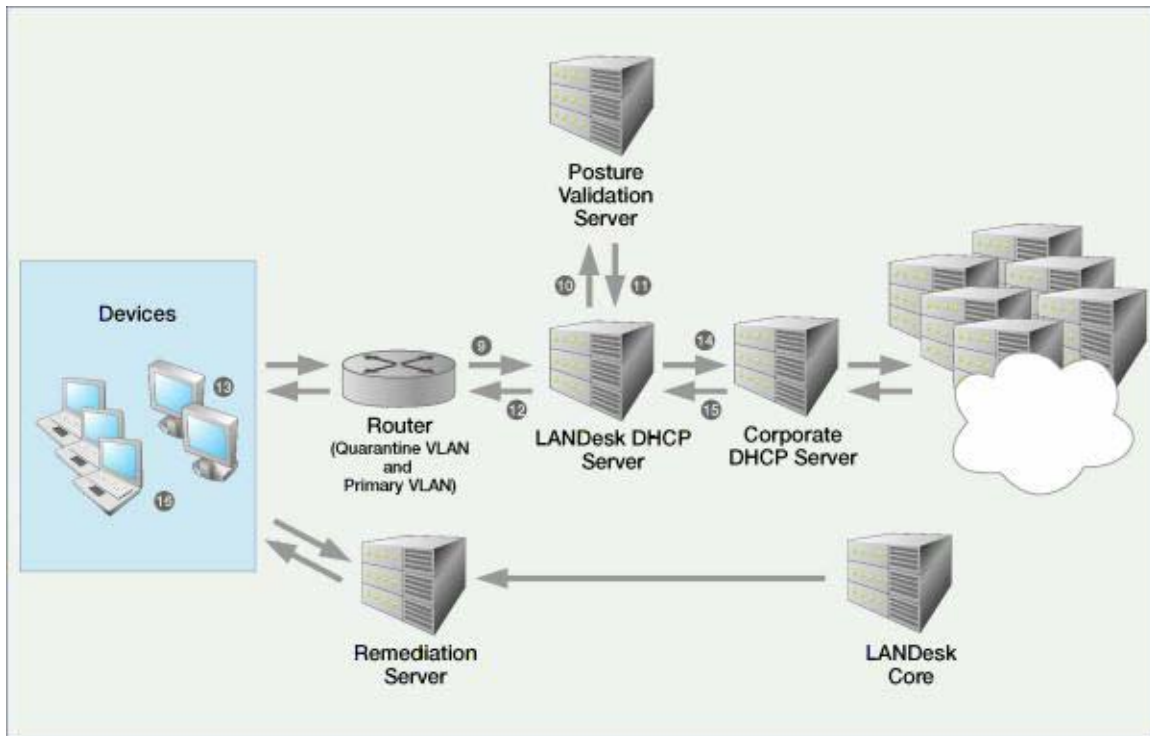
Phase 2: Remediated device access attempt (IP address reassigned; posture statement requested)



Process workflow for the second access attempt:

6. The remediated device attempts to access the network again via the LANDesk DHCP server and requests an IP address.
7. The LANDesk DHCP server considers the device to still be in a quarantined state, and so...
8. The LANDesk DHCP server returns the same Quarantine VLAN IP address to the device, and now queries the LTA on the device for a health posture statement.

Phase 3: Device posture validation (permanent IP address reassigned to healthy device; network access granted)



Process workflow for posture validation and network access:

9. The device send its posture statement (health status) back to the LANDesk DHCP server.
10. The LANDesk DHCP server forwards the device posture statement on to the posture validation server.
11. The posture validation server sends posture reply to the LANDesk DHCP server. (Note that it is the posture validation server that acts as the decision point in the network access control process, meaning it determines the posture or health status of the device seeking network access.)
12. The LANDesk DHCP server communicates the posture reply to the device.
13. If the device is considered unhealthy (or non-compliant), it remains in the quarantine VLAN. If the device is considered healthy (or compliant), the device again requests an IP address from the LANDesk DHCP server.
14. Now, the LANDesk DHCP server recognized the devices as being healthy and passes the IP address request on to the primary corporate DHCP server.
15. The primary corporate DHCP server notifies the LANDesk DHCP server about a permanent IP address being assigned to the healthy device, and...
16. The primary DHCP server returns the permanent IP address to the healthy device, and the device is granted access to the corporate network.

Network topology and design considerations for a LANDesk DHCP trusted access implementation

You should keep the following issues in mind when designing your LANDesk DHCP trusted access implementation:

- The LANDesk core server should not be visible to the quarantine network.
- The LANDesk DHCP server needs to be on the opposite side of the router/switch from the clients.
- The router needs to support a primary and secondary subnet for the client side of the router.
- The router needs to be configured to forward broadcasted BOOTP/DHCP requests to the LANDesk DHCP server (relay agent or IP helper).
- The primary DHCP server should be on the same side of the router as the LANDesk DHCP server.
- The LANDesk DHCP server can service many quarantined subnets, so potentially only one LANDesk DHCP server is required.
- Do not put the LANDesk DHCP server on the same box as the primary DHCP server; they cannot share the same ports.
- The remediation server and posture validation server can be installed on the same box as the LANDesk DHCP server machine, but if performance or scalability issues arise they can be moved to their own server machines.
- The router must be configured with the real subnet as the primary subnet and the quarantined subnet as the secondary subnet.
- The secondary subnet should be restricted to only be able to see the remediation server.

Installing the LANDesk Trust Agent on devices to enable compliance scanning

In order to communicate with the LANDesk DHCP server and the posture validation server, and to have its health posture evaluated, a device must have the LANDesk Trust Agent (LTA) installed.

Keep in mind that in order to provide additional device management capabilities, you can also install the LTA (which includes the inventory scanner and local scheduler) on managed devices even if you're using the Cisco NAC solution. In other words, you can have both trust agents installed on the device. However, if you're using the LANDesk DHCP solution, you should not install the CTA on managed devices.

Important note on installing the full standard LANDesk agent: You must have the full standard LANDesk agent installed on a device in order to avoid having healthy devices that leave your network automatically be granted access to the network without being scanned for security compliance the next time they connect to your network (thereby circumventing the posture validation process).

If a device has only the applicable trust agent installed (either CTA or LTA), they will be considered healthy and let back on the network without having their posture validated.

To prevent this from happening, install the full standard LANDesk agent as soon as possible on your devices.

To install the LANDesk Trust Agent on managed employee devices

- If they already have the standard LANDesk agent, install the LTA with a new device agent configuration
- Or, if they don't have the standard LANDesk agent, install the LTA with the initial agent configuration
- Or, install the LTA with an agent configuration to devices in UDD

To install the LANDesk Trust Agent on unmanaged employee devices

- Install the LTA by pulling with the standard LANDesk agent (wscfg32.exe)
- Or, by using a self-contained Agent Configuration

To install the LANDesk Trust Agent on new end user devices (employee or visitor)

- Install the LTA manually using a UNC or URL path (with the HowToInstall.html page located on the remediation Web share)

Setting up and configuring a posture validation server

This is a common component and therefore a common task for both the LANDesk DHCP and Cisco NAC trusted access solutions.

For more information and step-by-step instructions, see [Setting up and configuring a posture validation server](#).

Setting up and configuring a remediation server

This is a common component and therefore a common task for both the LANDesk DHCP and Cisco NAC trusted access solutions.

For more information and step-by-step instructions, see [Setting up a remediation server](#).

Setting up a LANDesk DHCP server

This is a unique procedure for the LANDesk DHCP solution. For detailed information (including configuring your router/switch for a LANDesk DHCP solution), see [Setting up a LANDesk DHCP server](#).

What you should do after setting up a LANDesk DHCP implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk Trusted Access is to: define your compliance security policy, and publish trusted access settings to posture validation servers and remediation servers. These tasks are the same and apply to both the LANDesk DHCP and the Cisco NAC solutions. For information on performing these tasks, see [Configuring compliance security and publishing trusted access settings](#).

Additionally, to learn more about other ongoing trusted access management tasks such as: ensuring trusted access services is enabled (turned on), using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing to posture validation servers and remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see [Managing compliance security](#).

Use this quickstart task list to complete the planning, setup, and configuration tasks required to get the LANDesk DHCP implementation of LANDesk Trusted Access up and running on your network.

You can print out this task list and refer to it to keep track of each step during the implementation process. If you're viewing this task list online, you can click the **For more information** link to view detailed information and instructions about that particular task.

Setting up a single trusted access server

For the purposes of this quickstart task list, the posture validation server, the remediation server, and the LANDesk DHCP server are all installed and configured on the same machine called the trusted access server. While this configuration is technically feasible and will create a functional LANDesk DHCP trusted access environment, keep in mind that it might not be the most suitable arrangement for your corporate network.

Quickstart task list for setting up a LANDesk DHCP implementation

Done	Task	For more information, go to
<input type="checkbox"/>	Prerequisite: A LANDesk Management Suite 8.6 core server must be installed and running on your network, activated with a LANDesk Security Suite license and security content subscriptions: <ul style="list-style-type: none"> • Install the core server • Activate the core with a Security Suite license • Log in as an Administrator user or as a user with both the Security and Patch Management and Security and Patch Compliance rights (allows downloading security and patch content and copying it to the Compliance group) 	Using Security and Patch Manager For information on LANDesk DHCP components and process workflow (including diagrams), see Understanding the LANDesk DHCP components and process workflow. For information on network topology and design considerations for a LANDesk DHCP trusted access implementation, see Network topology and design considerations for a LANDesk DHCP implementation.
<input type="checkbox"/>	Install the LANDesk Trust Agent (LTA) on devices to enable compliance scanning: <ul style="list-style-type: none"> • For managed employee devices: If they already have the standard LANDesk agent, install the LTA with a new device agent configuration Or, if they don't have the standard LANDesk agent, install the LTA with the initial agent configuration Or, install the LTA with an agent configuration to devices in UDD • For unmanaged employee devices: 	Installing the LANDesk Trust Agent on devices to enable compliance scanning

Install the LTA by pulling with the standard
 LANdesk agent (wscfg32.exe)
 Or, by using a self-contained Agent Configuration

- **For new end user devices (employee or visitor):**
 Install the LTA manually using a UNC or URL path
 (with the HowToInstall.html page located on the
 remediation Web share)

- | | |
|---|---|
| <p>❑ Identify and configure a single trusted access server that meets the following system requirements:</p> <ul style="list-style-type: none"> • Windows 2000 or above, with .NET Framework 1.1 • Web server installed and running (IIS) • Static IP address • The server must be on the opposite side of the router/switch from connecting devices • Can't be a current DHCP server • Can't be a PXE representative machine | |
| <p>❑ Setup a posture validation server:</p> <ul style="list-style-type: none"> • On the trusted access server (see above), • Run the setup program located in:
 <coreserver>\LDMain\Install\TrustedAccess\Postu
 reServer | <p>Setting up and configuring a posture validation server</p> |
| <p>❑ Setup a remediation server:</p> <ul style="list-style-type: none"> • On the trusted access server, • Create a Web share named LDLogon (typically at:
 c:\inetpub\wwwroot\LDLogon) • Use the IIS tool to: add a new MIME type for .Ird and set it to application/binary, and enable anonymous access with Read and Browse rights for the LDLogon share | <p>Setting up and configuring a remediation server</p> |
| <p>❑ Define compliance security with the Security and Patch Manager tool:</p> <ul style="list-style-type: none"> • In the console's Security and Patch Manager tool, • Download security content definitions and patches • Add security definitions to the Compliance group in order to define your compliance security policy • Make sure associated patches are downloaded | <p>Defining compliance security criteria in the Security and Patch Manager tool</p> |
| <p>❑ Configure the posture validation server:</p> <ul style="list-style-type: none"> • In Security and Patch Manager, right-click the Trusted Access group, and click Configure trusted access • Enter the posture validation server name, click Add to add it to the list, and then click OK | <p>Setting up and configuring a posture validation server</p> |
| <p>❑ Configure the remediation server:</p> | <p>Setting up and configuring a</p> |

- In Security and Patch Manager, right-click the Trusted Access group and click Configure remediation servers, and then click Add
 - Enter the remediation server IP address, the UNC path to the LDLogon Web share you've created on the remediation server where files are published, and user access credentials, and then click OK
- ☐ Publish ALL trusted access settings to appropriate servers: Publishing trusted access settings
 - In Security and Patch Manager, right-click the Trusted Access group and click Publish trusted access settings, and then select All
 - The initial publishing process must include ALL of the trusted access settings; subsequent publishing can include compliance content only
- ☐ Install the LANDesk DHCP plug-in on the primary DHCP server: Setting up a LANDesk DHCP server
 - Copy LDDHCPPlugin.dll and LDDHCPPlugin.reg from:
LDMain\Install\TrustedAccess\LDDHCP\Microsoft DHCP on the core server to any local folder on your primary Microsoft DHCP server
 - Edit the LDDHCPPlugin.reg file for the correct path and IP address to the LANDesk DHCP server
 - Import the LDDHCPPlugin.reg file into the registry
 - Restart the Microsoft DHCP service
- ☐ Setup and configure the LANDesk DHCP server: Setting up a LANDesk DHCP server
 - On the trusted access server,
 - Run the setup program located in:
<coreserver>\LDMain\Install\TrustedAccess\LDDHCP
(copy the setup program to a disk if the core can't be accessed)
 - Copy keys and certificate files (*.key, *.crt) from the core server's Program Files\LANDesk\Shared Files\Keys folder to the same file path on the LANDesk DHCP server
 - Configure LANDesk DHCP server settings with the LDDHCP Configuration tool that can be accessed by the shortcut icon located on the desktop
 - Check the Allow Access to Everyone option
 - Enter posture validation server information
 - Create VLAN address pool scopes for each subnet (make sure to define at least the scope option 003 for the router gateway)
 - Exit the Configuration tool to start the LANDesk DHCP service
- ☐ Configure your router for LANDesk DHCP trusted access: LANDesk DHCP server prerequisites: Network and

- The router must be located between the LANDesk DHCP server and connecting devices router configuration requirements
 - The router must have DHCP forwarding turned on
 - Add a VLAN subnet to the client interface on the router (the quarantine subnet)
 - Change the IP address helper (relay agent) on the client interface to point to the LANDesk DHCP server
 - Add ACL rules on the router to restrict traffic from the VLAN so that devices can only reach the remediation server
- ☐ Ensure the posture validation process is working properly:
- Try a simple test with the LANDesk DHCP trusted access network you've just set up by releasing and renewing a managed device's IP address.
- ☐ Perform ongoing compliance security management tasks: Managing compliance security
- Ensuring trusted access services is enabled (turned on)
 - Using the allow/restrict access to everyone option
 - Understanding what happens when connecting devices are postured
 - Viewing affected (non-compliant) devices
 - Modifying and updating compliance security policies
 - Adding unmanaged devices
 - Configuring and viewing compliance logging
 - Generating compliance reports

To return to the main help topic for the LANDesk DHCP trusted access, see [Using the LANDesk DHCP solution](#).

This chapter describes how to plan, set up, configure, and enable the Cisco NAC implementation of LANDesk Trusted Access.

With the Cisco NAC solution, you can take advantage of existing Cisco hardware, software, agents, protocols, and posture evaluation processes that might already be a part of your network infrastructure. For detailed information about the Cisco router, servers, and NAC technologies you should refer to your official Cisco documentation.

Audience disclaimer and assumptions

"The intended audience for setting up Cisco NAC consists of system engineers and network administrators responsible for the implementation of Cisco NAC. This document assumes you are familiar with Microsoft Windows operating systems and client machines and with the configuration and operation of Cisco Secure ACS. It also assumes you know how to configure Cisco IOS devices, and are familiar with certificate authorities and the trust models provided by digital certificates."

The note above is taken from the official Cisco document entitled "Implementing Network Admission Control Phase One Configuration and Deployment."

In addition to the specific Cisco components, you must also set up a posture validation server and a remediation server in order to implement LANDesk Trusted Access.

Read this chapter to learn about:

Setting up a Cisco NAC implementation of trusted access

- Quickstart task list for setting up a Cisco NAC implementation
- Understanding the Cisco NAC components and process workflow
- Network topology and design considerations for a Cisco NAC implementation
- Setting up a Cisco router
- Setting up a Cisco Secure Access Control Server (ACS)
- Installing the Cisco Trust Agent on devices to enable compliance scanning
- Setting up and configuring a posture validation server
- Configuring a connection between the posture validation server and the Cisco ACS
- Setting up and configuring a remediation server

What you should do after setting up a Cisco NAC implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk Trusted Access is to: define your compliance security policy, and publish trusted access settings to posture validation servers and remediation servers. These tasks are the same and apply to both the LANDesk DHCP and the Cisco NAC solutions. For information on performing these tasks, see *Configuring compliance security and publishing trusted access settings*.

Additionally, to learn more about other ongoing trusted access management tasks such as: ensuring trusted access services is enabled (turned on), using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing to posture validation servers and remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see *Managing compliance security*.

Quickstart task list for setting up a Cisco NAC implementation

Use this task checklist to help keep track of the steps required to set up the Cisco NAC solution: Quickstart task list for setting up a Cisco NAC implementation.

Understanding the Cisco NAC components and process workflow

This section describes the components that comprise a Cisco NAC solution. Additionally, this section describes what happens when a device attempts to access or connect to the corporate network when LANDesk Trusted Access is enabled. Scenarios with and without a Cisco Trust Agent (CTA) installed on the device are covered in the diagrams and process workflows below.

The following components are required for the Cisco NAC-based LANDesk trusted access service.

Required components

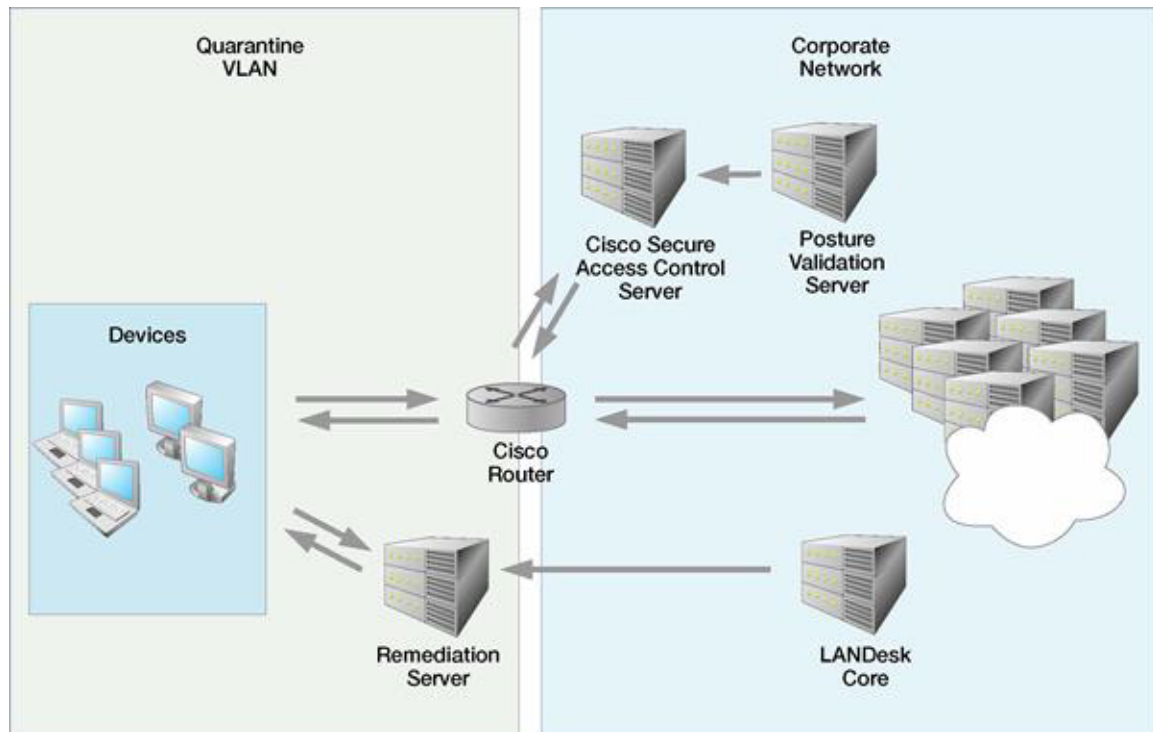
Component	Description
LANDesk core server	Provides the Security and Patch Manager tool used to: download security content (such as OS and application vulnerability definitions, spyware definitions, system configuration security threats, antivirus and firewall configuration definitions, etc.), define compliance criteria, configure posture validation servers and remediation servers, and configure and publish trusted access settings (including compliance security rules or policies and remediation resources for scanning and repairing devices).
Corporate DHCP server	Provides permanent IP addresses to devices.
Posture validation server	Determines whether the connecting device has a healthy or unhealthy posture based on two factors: your compliance security policy (the contents of the Compliance group in the Security and Patch Manager tool) AND the number of hours since a healthy scan as specified in the Definition of healthy setting in the Configure trusted access dialog. The posture validation server is the policy decision point in the validation process.
Remediation server	Contains the necessary setup and support files (security client, security type definitions and required patches, as well as the HTML template pages) used to scan devices for vulnerabilities identified by your security policy and remediate (repair) any detected vulnerabilities so that the device can be scanned as healthy or compliant and access the network.
Cisco router	Acts as a network access device that enforces the compliance security policy. Communicates with both the connecting device attempting access and the Cisco Secure ACS to evaluate the posture credentials of the endpoint device. In other words, in a Cisco NAC environment the router is the policy enforcement point on the network and grants or denies access privileges.
Cisco Secure ACS	Cisco specific hardware device that acts as the primary posture validation server in a Cisco NAC environment. Contains the ACLs (Access Control Lists) that define posture enforcement rules. With LANDesk trusted access, the Cisco Secure ACS is configured to delegate posture decisions to the posture validation server (or servers) you set up and configure on the network.
Devices	Mobile or guest user devices, as well as regular network user devices, attempting to access your corporate network. Typical

endpoint devices include desktop computers and laptops but may also be "clientless" devices such as printers, etc. LANDesk Trusted Access allows you to evaluate the health status of these connecting devices and control network access based on their posture credentials.

The following diagrams show a typical configuration of the components described above, as well as the posture validation process or workflow between those components.

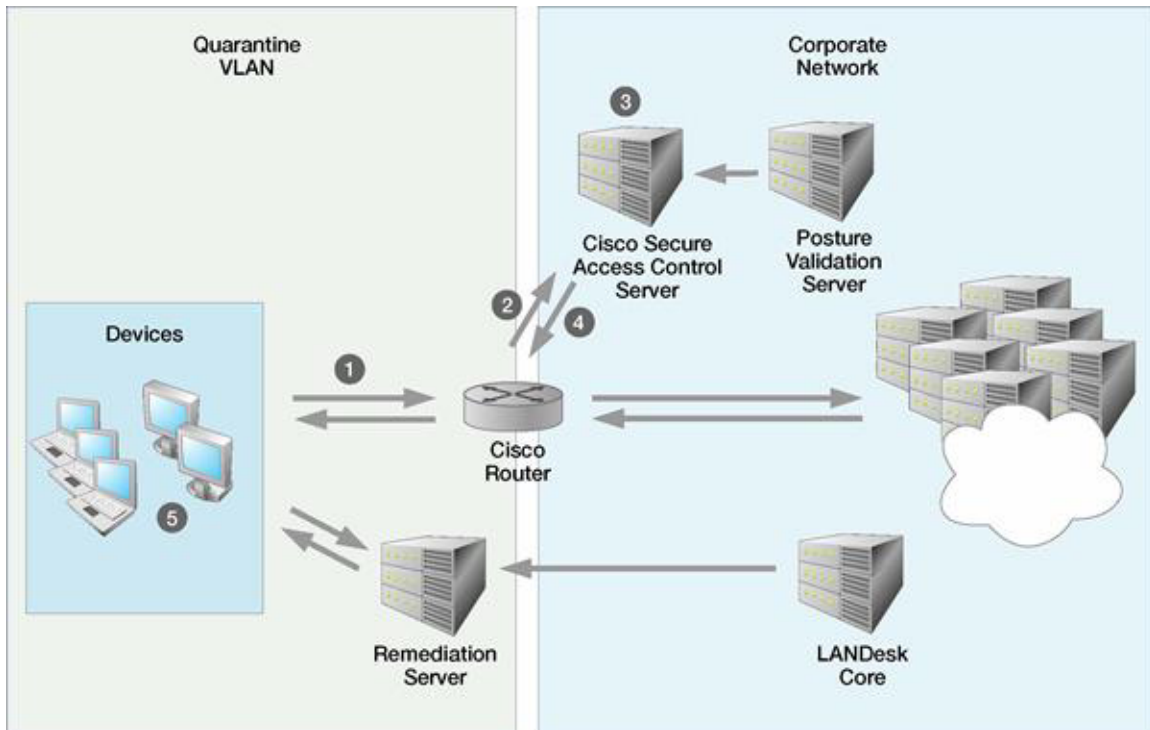
Cisco NAC components

The diagram below shows the specific Cisco NAC components.



Posture validation process for a device without the CTA installed

The diagram below shows the workflow or communication flow between the various components in a Cisco NAC environment when the device attempting to access the network does not have the Cisco Trust Agent installed. The callout numbers represent each stage of the process and are explained in the steplist below.

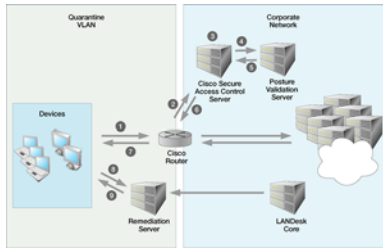


Process workflow:

1. A device that is NOT configured with the Cisco Trust Agent (CTA) makes an initial attempt to log in to the corporate network via the Cisco router.
2. The router forwards the device access request to the Cisco Secure Access Control Server (ACS) containing Access Control Lists (ACLs) defined by the administrator that determine access rights for each posture or health status.
3. Because the trust agent (CTA) isn't installed on the device, the Cisco ACS can't determine its posture or health status and doesn't forward the device access request to the posture validation server.
4. The Cisco ACS automatically rejects the "clientless" access attempt, and forwards the appropriate ACL on to the router.
5. According to the ACL (as defined by the administrator), a device in this situation is typically restricted to the quarantine VLAN and has no access to the corporate network at this point. The user can choose whether to remain in the quarantine VLAN or take the steps necessary to demonstrate compliance with the network's security policy and gain full network access. In order to gain network access, first the CTA must be manually installed (via a UNC path or URL to the CTA setup program), and then the device must access the remediation server in order to install the LANDesk Security Client that performs vulnerability assessment scanning and remediation. Once the device is repaired, the network access process is repeated and the healthy (i.e., compliant) device is granted access to the corporate network.

Posture validation process for a device with the CTA installed

The diagram below shows the workflow or communication flow between the various components in a Cisco NAC environment when the device attempting to access the network has the Cisco Trust Agent installed. The callout numbers represent each stage of the process and are explained below.



Process workflow:

1. A device that is configured with the Cisco Trust Agent (CTA) makes an initial attempt to log in to the corporate network via the Cisco router.
2. The router forwards the device access request to the Cisco Secure Access Control Server (ACS) containing Access Control Lists (ACLs) defined by the administrator that determine access rights for each posture or health status.
3. Because the trust agent is installed on the device (and a connection between the posture validation server and the Cisco ACS has been configured), the Cisco ACS can forward the device access request to the posture validation server.
4. The posture validation server determines the health status or "posture" of the device against a security policy comprised of compliance rules or credentials predefined by the LANDesk administrator with the Compliance feature of the Security and Patch Manager tool. These compliance rules are published from the core server to the posture validation server. (Note that it is the posture validation server that acts as the decision point in the network access control process, meaning it determines the posture or health status of the device seeking network access.)
5. The posture validation server sends a posture statement (or token) for that particular device back to the Cisco ACS.
6. The Cisco ACS forwards the appropriate ACL (depending on the posture statement) on to the router.
7. The posture statement is communicated back to the trust agent on the device in the quarantine area. If the device is considered healthy (or compliant), it is granted access to the corporate network.
8. However, if the device is considered unhealthy (or non-compliant) it remains in the quarantine VLAN. A message box displays informing the user how to contact the remediation server in order to install the LANDesk Security Client that performs vulnerability assessment scanning and remediation. The user can choose whether to remain in the quarantine VLAN or take the steps necessary to demonstrate compliance with the network's security policy and gain full network access.
9. Remediation is performed by the remediation server by scanning for vulnerabilities and other security risks (the compliance rules mentioned above) and installing any required patches. Once the device is repaired, the network access process is repeated and the healthy (i.e., compliant) device is granted access to the corporate network.

Network topology and design considerations for a Cisco NAC implementation

You should keep the following issues in mind when designing your Cisco NAC trusted access implementation:

- The LANDesk core server should not be visible to the quarantine network.
- The remediation server and posture validation server (and the Cisco ACS for that matter) can be installed on the same machine, but if performance or scalability issues arise they can be moved to their own server machines.

- The router needs to support a primary and secondary subnet for the client side of the router.
- The router must be configured with the real subnet as the primary subnet and the quarantined subnet as the secondary subnet.
- The secondary subnet should be restricted to only be able to see the remediation server.

Setting up a Cisco router

The Cisco NAC trusted access solution assumes a Cisco router on your network.

If you don't already have a Cisco router set up on your network and you want to use the Cisco NAC solution, LANDesk does offer some router setup information on its support Web site.

For detailed Cisco router setup information

You can view detailed setup instructions for a typical Cisco router to be used in a Cisco NAC trusted access environment on the LANDesk Software support Web site.

We also strongly recommend that you refer to your Cisco router documentation for more detailed instructions on setting up the router.

Setting up a Cisco Secure Access Control Server

The Cisco NAC trusted access solution also assumes a Cisco Secure Access Control Server (ACS) on your network. The Cisco ACS is where you define posture credentials and configure external databases (such as a posture validation server) to communicate and resolve device posture status during the posture validation process.

If you don't already have a Cisco Secure ACS set up on your network and you want to use the Cisco NAC solution, LANDesk does offer some Cisco Secure ACS setup information on its support Web site.

For detailed Cisco Secure Access Control Server (ACS) setup information

You can view detailed setup instructions for a Cisco Secure ACS router to be used in a Cisco NAC trusted access environment on the LANDesk Software support Web site.

We also strongly recommend that you refer to your Cisco router documentation for more detailed instructions on setting up the router.

Installing the Cisco Trust Agent on devices to enable compliance scanning

In order to communicate with the Cisco Secure ACS and have its health posture evaluated, a device must have the Cisco Trust Agent (CTA) installed.

Manually installing the Cisco Trust Agent (CTA)

For Cisco NAC, the trust agent (CTA) must be installed manually, on both managed and unmanaged devices, from the core server using a UNC or URL path. You can use the HowToInstallCisco.html file located on the remediation Web share to install the CTA.

Keep in mind that in order to provide additional device management capabilities, you can also install the LTA (which includes the inventory scanner and local scheduler) on managed devices even if you're using the Cisco NAC solution. In other words, you can have both trust agents installed on the device. However, if you're using the LANDesk DHCP solution, you should not install the CTA on managed devices.

Important note on installing the full standard LANDesk agent: You must have the full standard LANDesk agent installed on a device in order to avoid having healthy devices that leave your network automatically be granted access to the network without being scanned for security compliance the next time they connect to your network (thereby circumventing the posture validation process).

If a device has only the applicable trust agent installed (either CTA or LTA), they will be considered healthy and let back on the network without having their posture validated.

To prevent this from happening, install the full standard LANDesk agent as soon as possible on your devices.

To install the Cisco Trust Agent on managed and unmanaged devices

1. From the device, create a UNC mapping to the location of the HowToInstallCisco.html file. This HTML page should already be copied to a Web share on the remediation server. (This is the location you specified when you configured the remediation server in the **Location to copy compliance files** field.)
2. Or, open the device's browser and enter the URL to the HowToInstallCisco.html file located on the remediation server.
3. Follow the instructions on the page that displays.
4. When the CTA is installed, you can click the link to scan your computer for compliance, and then follow the instructions to gain Internet access only or to gain full access to the corporate network by installing the necessary security client.

Setting up and configuring a posture validation server

This is a common component and therefore a common task for both the LANDesk DHCP and Cisco NAC trusted access solutions.

For more information and step-by-step instructions, see [Setting up and configuring a posture validation server](#).

Configuring a connection between the posture validation server and the Cisco Secure ACS

This is a unique procedure for the Cisco NAC solution.

For more information and step-by-step instructions, see [Setting up communication between a posture validation server and the Cisco Secure ACS](#).

Setting up and configuring a remediation server

This is a common component and therefore a common task for both the LANDesk DHCP and Cisco NAC trusted access solutions.

For more information and step-by-step instructions, see [Setting up and configuring a remediation server](#).

What you should do after setting up a Cisco NAC implementation

After you've completed the setup tasks listed above, the next step in implementing LANDesk Trusted Access is to: define your compliance security policy, and publish trusted access settings to posture validation servers and remediation servers. These tasks are the same and apply to both the LANDesk DHCP and the Cisco NAC solutions. For information on performing these tasks, see [Configuring compliance security and publishing trusted access settings](#).

Additionally, to learn more about other ongoing trusted access management tasks such as: ensuring trusted access services is enabled (turned on), using the allow/restrict access to everyone option, understanding what happens when connecting devices are postured, updating compliance security rules and policies and republishing to posture validation servers and remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see [Managing compliance security](#).

Use this task list to complete the planning, setup, and configuration tasks required to implement the Cisco NAC trusted access solution on your LANDesk network.

You can print this task list and refer to it to track each step during the implementation process. If you're viewing this task list online, click the **For more information** link to view detailed information for a particular task.

Setting up a single trusted access server

For the purposes of this quickstart task list, the posture validation server and the remediation server are installed and configured on the same machine called the trusted access server. While this configuration is technically feasible and will create a functional trusted access environment, keep in mind that it might not be the most suitable arrangement for your corporate network.

Quickstart task list for setting up a Cisco NAC implementation

Done	Task	For more information, go to
<input type="checkbox"/>	Prerequisite: A LANDesk Management Suite 8.6 core server must be installed and running on your network, activated with a LANDesk Security Suite license and security content subscriptions: <ul style="list-style-type: none"> • Install the core server • Activate the core with a Security Suite license • Log in as an Administrator user or as a user with both the Security and Patch Management and Security and Patch Compliance rights (allows downloading security and patch content and copying it to the Compliance group) 	<p>Using Security and Patch Manager</p> <p>For information on the Cisco NAC components and process workflow (including diagrams), see Understanding the Cisco NAC components and process workflow.</p> <p>For information on network</p>

topology and design considerations for a Cisco NAC trusted access implementation, see Network topology and design considerations for a Cisco NAC implementation.

- | | |
|---|---|
| <input type="checkbox"/> Set up a Cisco router: <ul style="list-style-type: none"> • If a router is not already set up, the recommendation is to access the LANDesk Support site for basic instructions, and refer to Cisco documentation | Setting up a Cisco router |
| <input type="checkbox"/> Set up a Cisco Secure Access Control Server (ACS): <ul style="list-style-type: none"> • If a Cisco Secure ACS is not already set up, the recommendation is to access the LANDesk Support site for basic instructions, and refer to Cisco documentation | Setting up a Cisco Secure Access Control Server (ACS) |
| <input type="checkbox"/> Install the Cisco Trust Agent (CTA) on devices to enable compliance scanning: <ul style="list-style-type: none"> • For all devices including managed, unmanaged, and new devices: Install the CTA manually using a UNC or URL path (with the HowToInstall.html page located on the remediation Web share) | Installing the Cisco Trust Agent on devices to enable compliance scanning |
| <input type="checkbox"/> Identify and configure a single trusted access server that meets the following system requirements: <ul style="list-style-type: none"> • Windows 2000 or above, with .NET Framework 1.1 • Web server installed and running (IIS) • Static IP address • The server must be on the opposite side of the router/switch from connecting devices • Can't be a current DHCP server • Can't be a PXE representative machine | |

- | | |
|--|---|
| <input type="checkbox"/> Setup a posture validation server: <ul style="list-style-type: none"> • On the trusted access server (see above), • Run the setup program located in:
<coreserver>\LDMain\Install\TrustedAccess\Postu
reServer | Setting up and configuring a posture validation server |
| <input type="checkbox"/> Configuring a connection between the posture validation server and the Cisco Secure ACS: <ul style="list-style-type: none"> • This procedure applies only to the Cisco NAC solution, and step-by-step instructions are provided in the topic referenced to the right. | Configuring a connection between the posture validation server and the Cisco Secure ACS |
| <input type="checkbox"/> Setup a remediation server: <ul style="list-style-type: none"> • On the trusted access server, • Create a Web share named LDLogon (typically at: c:\inetpub\wwwroot\LDLogon) • Use the IIS tool to: add a new MIME type for .lrd and set it to application/binary, and enable anonymous access with Read and Browse rights for the LDLogon share | Setting up and configuring a remediation server |
| <input type="checkbox"/> Define compliance security with the Security and Patch Manager tool: <ul style="list-style-type: none"> • In the console's Security and Patch Manager tool, • Download security content definitions and patches • Add security definitions to the Compliance group in order to define your compliance security policy • Make sure associated patches are downloaded • Define healthy and unhealthy postures in the console's trusted access dialog | Defining compliance security criteria in the Security and Patch Manager tool |
| <input type="checkbox"/> Configure the posture validation server: <ul style="list-style-type: none"> • In Security and Patch Manager, right-click the Trusted Access group, and click Configure trusted access • Enter the posture validation server name, click Add to add it to the list, and then click OK | Setting up and configuring a posture validation server |

- | | |
|---|---|
| <input type="checkbox"/> Configure the remediation server: <ul style="list-style-type: none"> • In Security and Patch Manager, right-click the Trusted Access group and click Configure remediation servers, and then click Add • Enter the remediation server IP address, the UNC path to the LDLogon Web share you've created on the remediation server where files are published, and user access credentials, and then click OK | Setting up and configuring a remediation server |
| <input type="checkbox"/> Publish ALL trusted access settings to appropriate servers: <ul style="list-style-type: none"> • In Security and Patch Manager, right-click the Trusted Access group and click Publish trusted access settings, and then select All • The initial publishing process must include ALL of the trusted access settings; subsequent publishing can include compliance content only | Publishing trusted access settings |
| <input type="checkbox"/> Ensure the posture validation process is working properly: <ul style="list-style-type: none"> • Try a simple test with the Cisco NAC trusted access network you've just set up by releasing and renewing a managed device's IP address. | |
| <input type="checkbox"/> Perform ongoing compliance security management tasks: <ul style="list-style-type: none"> • Ensuring trusted access services is enabled (turned on) • Using the allow/restrict access to everyone option • Understanding what happens when connecting devices are postured • Viewing affected (non-compliant) devices • Modifying and updating compliance security policies • Adding unmanaged devices • Configuring and viewing compliance logging • Generating compliance reports | Managing compliance security |

To return to the main help topic for Cisco NAC trusted access, see [Using the Cisco NAC solution](#).

A posture validation server is required for both LANDesk Trusted Access solutions: LANDesk DHCP and Cisco NAC.

The posture validation server evaluates a device's health posture statement against the compliance security rules defined in the Security and Patch Manager tool in the console, and then returns a health posture to the device via the router or the LANDesk DHCP server depending on which trusted access solution you've implemented.

In a LANDesk DHCP trusted access environment, the posture validation server communicates the posture statement via the LANDesk DHCP server. In a Cisco NAC trusted access environment, the posture validation server communicates the device's posture statement (or health status) via the Cisco Secure Access Control Server (ACS). See the relevant component and process diagrams in *Using the LANDesk DHCP solution*, and *Using the Cisco NAC solution*.

You can have more than one posture validation server on your network.

Read this chapter to learn about:

Setting up and configuring a posture validation server

- Posture validation server prerequisites
- Determining server location on the network
- Running the server setup program
- Configuring (adding) posture validation servers in the console
- Next steps: Publishing compliance rules to posture validation servers
- Configuring a connection between the posture validation server and the Cisco ACS (Cisco NAC only)

Posture validation server prerequisites

The machine you set up as a posture validation server must meet the following system requirements:

- Windows 2000 server, Windows 2003 server, Windows XP
- .NET Framework installed (version 1.1)
- The posture validation server can be combined onto another machine such as the LDMS core server or the LANDesk DHCP server.

Determining the server location on the network

The posture validation server can be installed on the LDMS core server, the LANDesk DHCP server, or the primary DHCP server. However, if you have performance or scalability concerns then this should be installed on a separate server machine.

It is recommended that you use an IP address to identify a posture validation server.

If installed on a dedicated machine, the posture validation server should be accessible by the LANDesk core server and the LANDesk DHCP server or Cisco Secure ACS server.

You should have only one posture validation server per LANDesk DHCP server (LANDesk DHCP solution only).

You can see diagrams showing the component location and process workflow for each LANDesk Trusted Access solution in their respective overview sections. See, *Using the LANDesk DHCP solution*, and *Using the Cisco NAC solution*.

Running the server setup program

The setup files for posture validation servers are copied to the LANDesk core server during the main installation process. You set up a posture validation server using those setup files.

To set up the posture validation server

1. Map a drive from the machine you want to set up as a posture validation server to the LDMain folder on your core server. Navigate to the \Install\TrustedAccess\PostureServer folder.
2. Run the postureserversetup.exe program.
3. At the **Welcome** screen, click **Next**.
4. Accept the license agreement, and then click **Next**.
5. To copy the necessary files, click **Install**.
6. When the file copy process is complete, click **Finish**.

The posture server setup program copies files, starts the posture server service, and listens for incoming requests on TCP ports 4444 and 12576 (the default ports). You should ensure that any firewalls are open.

The posture validation server is now ready to be configured in the console.

Important additional task for Cisco NAC only

For a Cisco NAC implementation, you also have to configure a connection between the posture validation server and the Cisco Secure ACS. This connection allows the posture validation server to send posture statements to the ACS for devices attempting to access the network based on the security compliance criteria. For more information, see *Configuring a connection between the posture validation server and the Cisco ACS (Cisco NAC only)* below.

For a LANDesk DHCP implementation, this procedure is not relevant because the posture validation server communicates with connecting devices through the LANDesk DHCP server.

Configuring (adding) posture validation servers in the console

Once a posture validation server is set up, you must add it to the list of valid posture validation servers in the **Configure trusted access** dialog in the console. This allows the core server to configure and communicate with (publish compliance rules) the posture validation server.

To add posture validation servers in the console

1. In the Security and Patch Manager tool window, right-click the **Trusted Access** group, and then click **Configure trusted access**.
2. To add posture validation server(s) to your network, enter the IP address of a posture validation server in the field provided, and then click **Add**.
3. Click **OK**.

You can now publish trusted access content to the server (as long as you've also configured a remediation server and user credentials).

About the Configure Trusted Access dialog

Use this dialog to define healthy and unhealthy posture, configure logging, add posture validation servers, and publish trusted access settings to the posture validation servers on your network.

Note: You must first set up these components before you can add them with this dialog.

- **Definition of healthy:** Indicates the number of hours since the last compliance security scan that didn't detect any vulnerabilities (as defined by the contents of the Compliance group in Security and Patch Manager) on the scanned device.
- **Definition of unhealthy:** Indicates the default unhealthy posture that determines whether the scanned device is unhealthy. Default postures are defined by the Access Control Lists in the Cisco NAC implementation.
- **Minimum logging level:** Indicates the logging level for the posture validation server log files.
- **Posture validation server name:** Enter a name in this field, and click **Add** to add posture validation servers to your network. For information on setting up posture servers, see Setting up a posture validation server. When you publish trusted access settings, they are published to all of the servers included in this list.
- **Audit for reporting only (Cisco only):** Allows everyone access to the network, whether their posture is determined to be healthy or unhealthy. This option is checked by default. Use this option if you're using the Cisco NAC trusted access implementation and want to allow everyone access to the network. This option doesn't apply to the LANDesk DHCP trusted access.
(Note: You can use this option to allow time to finalize the configuration of your trusted access network and compliance security policy, to let the regular Security and Patch Management process bring the majority of your managed devices into compliance, to observe the various trusted access logs and reports, and to choose the right time to begin enforcing a compliance security policy and restricting network access. Once the majority of managed devices are compliant, or whenever you as the network administrator feels it is time, unchecking this option enables trusted access on your network and blocks network access to devices that are found to be non-compliant.)
- **Publish:** Opens the **Publish trusted access settings** dialog that lets you specify which content you want to publish to posture validation servers and remediation servers. Any time you change the trusted access settings, you must republish the new settings to the posture validation servers.
(Note: Publishing trusted access content sends trusted access settings and compliance rules to posture validation servers AND any associated patches to remediation servers. Publishing Infrastructure files sends setup and support files, including the security client scanner and trust agents as well as the HTML template pages, to remediation servers.

Next steps: Publishing compliance rules to posture validation servers

The next step in setting up and configuring a posture validation server is to publish compliance rules (trusted access settings) to the posture validation servers. You must first define your compliance security criteria in the Security and Patch Manager tool before you can publish to servers.

For information about these tasks, see Configuring compliance security and publishing trusted access settings.

Configuring a connection between the posture validation server and the Cisco ACS (Cisco NAC only)

This task applies only to the Cisco NAC implementation of LANDesk trusted access.

For Cisco NAC, you must configure this connection between the posture validation server and the Cisco ACS so that they can communicate during the posture validation process when determining the posture or health status of a device attempting to connect to the network. As stated above, this procedure isn't relevant if you're using the LANDesk DHCP solution.

To configure a connection between the posture validation server and the Cisco Secure ACS

1. Copy the file named landeskattributes.txt (located on the core server in the C:\ProgramFiles\LANDesk\ManagementSuite\Install\TrustedAccess\Cisco folder to the C:\ drive of your Cisco Secure ACS.
2. On the Cisco Secure ACS, open a CMD.exe window and run the following command:
C:\ProgramFiles\CiscoSecure ACS v3.3\Utils\csutil -addAVP c:\landeskattributes.txt
3. Stop and restart the following services on the Cisco ACS:
 - csauth
 - csadmin
 - csutil
4. The LANDesk attributes will now appear in the Available Credentials list.
5. Launch the Cisco Secure ACS console.
6. Click **External User Database | Database Configuration | Network Admission Control | Create a New Configuration**.
7. Enter a name for the new configuration, and then click **Submit**.
8. In the External User Database Configuration box, click **Configure**.
9. In the Mandatory Credential Type box, click **Edit List**.
10. If you ran the batch file mentioned above, the Available Credentials list should show the Landesk.LDSS credentials. Move this object to the Selected Credentials list, and then click **Submit**.
11. In the Credential Validation Policies box, click **External Policies | New External Policy**.
12. Enter the name: PVS1
13. Enter a description.
14. Enter the URL: http://<posture validation server name:12576/pvs.exe
15. Set the timeout to 30 seconds.
16. Check the **Primary Server Configuration** check box.
17. In the Forwarding Credential Types box, move the Landesk.LDSS from the Available Credentials list to the Selected Credentials list, and then click **Submit**.
18. Add the PVS1 policy to the Selected Policies list, and then click **Submit**.
19. Click **Save Configuration**.

You've now completed the tasks that are specific to the Cisco Secure ACS component required in setting up a Cisco NAC implementation of LANDesk trusted access. For a complete list of all the tasks required in setting up a Cisco NAC environment, see the Quickstart task list for setting up a Cisco NAC environment.

To return to the main help topic for Cisco NAC trusted access, see Using the Cisco NAC solution.

To return to the main help topic for LANDesk DHCP trusted access, see Using the LANDesk DHCP solution.

Setting up and configuring a remediation server

Both of the LANDesk Trusted Access solutions (LANDesk DHCP and Cisco NAC) require a remediation server to repair vulnerable or infected devices. The remediation server is where a device whose posture is determined to be unhealthy is sent to be remediated (repaired) so that it can meet the compliance rules you've configured for a healthy status.

The remediation server is where you publish remediation resources, such as: the security clients (that scan for vulnerabilities and other security risks on devices), patch files, and the HTML pages that appear on devices providing options for remediation or limited network access. To understand how the remediation server interacts with the other trusted access components and connecting devices, see the relevant component and process diagrams in *Using the LANDesk DHCP solution*, and *Using the Cisco NAC solution*.

Read this chapter to learn about:

Setting up and configuring a remediation server

- Remediation server prerequisites
- Determining server location on the network
- Creating a Web share on the remediation server
- Configuring (adding) a remediation server in the console
- Next steps: Publishing infrastructure files to remediation servers

Remediation server prerequisites

The machine you want to set up as a remediation server must meet the following system requirements:

- The remediation server can be any type of Web server. For example: IIS on Windows, or Apache on Linux.
- You must create a Web share on the remediation server that has anonymous access with read and browse rights enabled. See *Creating a Web share on the remediation server* below for instructions.
- **Note:** If you're using an Apache Web server on Linux, the share you create must be a Samba share.

Determining server location on the network

The remediation server can be placed on either side of the router.

If you choose to have it on the client side of the router, then it will be more secure because you don't have to make any exceptions in your router rules, but you will have to manually walk all the remediation files to the machine each time you change them.

If you put it on the opposite side of the router, then you have a potential security risk since quarantine machines are accessing a machine on your network, but you can push remediation files to the machine without having to walk them there.

The remediation server must be visible from the remediation VLAN.

You can have more than one remediation server on your network.

You can see diagrams showing the component location and process workflow for each LANDesk Trusted Access solution in their respective overview sections. See, Using the LANDesk DHCP solution, and Using the Cisco NAC solution.

Creating a Web share on the remediation server

The Web share you create on the remediation server acts as a storage area for the patch executable files that are used to remediate vulnerabilities on affected devices. When you publish Infrastructure files or remediation resources (i.e., security client, patch files, and HTML files) from the core server, those files are copied to this Web share you create.

The name of the Web share must be LDLogon. You can create this share anywhere on the Web server. A typical path would be: C:\inetpub\wwwroot\LDLogon. However, you can create the share at any path as long as the URL redirect is configured to go to: http://servername/LDLogon.

After you create the Web share, you specify this path to the share when you're configuring the remediation server in the console (see Configuring a remediation server in the console below). This ensure the core server publishes remediation resources to the correct location on the remediation server.

To create and configure a Web share on the remediation server

1. At the remediation Web server, create a Web share named LDLogon where you want to publish remediation resources. You can choose any location on the Web server, but the URL redirect must go to: http://servername/LDLogon.
2. Right-click the share you just created, and then click **Properties**.
3. Click the **Web Sharing** tab, and then click the **Share this folder** option. The **Edit Alias** dialog displays.
4. In the **Access permissions** area, make sure that the Read, Write, and Directory browsing permissions are checked (selected). Leave the other options at their default values, and then click **OK**. If you see a warning prompt, click **OK** again. The folder should now appear in the **Aliases** list.
5. Make sure that **Default Web Site** is selected in the **Share on** field, and then click **OK** to save your settings and close the dialog.
6. (Optional) If the Web server is on a Windows 2003 server, you need to add a new MIME type for .lrd files, and set it to application/binary.

The remediation server is now ready to be configured (added) in the console.

Configuring (adding) a remediation server in the console

Once a remediation server is set up, you must configure and add it to the list of valid remediation servers in the **Configure remediation servers** dialog in the console. By doing this, the remediation server is recognized on the network and can communicate properly with the other trusted access components.

To configure and add remediation servers in the console

1. From the Security and Patch Manager tool in the console (**Tools | Security | Security and Patch Manager**), right-click the **Trusted Access** group, click **Configure remediation servers**, and then click **Add**. The **Remediation server name and credentials** dialog displays.

2. Enter the IP address of the remediation server.
3. Enter the path to the Web share (on the Web server you're setting up as a remediation server) where you want to publish compliance files. The Web share must be named LDLogon. Compliance files are the security definition files that define your compliance security policy (i.e., the contents of the **Compliance** group in Security and Patch Manager), as well as the required patch files that remediate detected vulnerabilities.

You can enter a UNC path or a mapped drive path. A UNC path is the most reliable method because drive mappings may change (see note below). You can click the Browse button to navigate to the share you want to publish compliance files to on the remediation server.

Important: If you enter a local path or a mapped drive in the Location to copy compliance files field, the files are published either to the local machine or to the specified mapped drive on the machine where the publish action is initiated. To ensure that compliance files are published to the same location on each remediation server on the network, we recommend using a UNC path to a network share.

4. Enter a valid user name and password to access the remediation server.
5. Click **OK** to add this remediation server to the list.

You can now publish remediation infrastructure files to the server (as long as you've also configured a posture validation server and user credentials).

About the Remediation server name and credentials dialog

Use this dialog to identify the remediation server and the path to Web share on the remediation server where remediation resources (security clients, patch files, and HTML pages) are published.

- **Remediation server name:** Identifies the remediation server by its IP address or hostname.
- **Location to copy compliance files:** Specifies the full path to the Web share located on the remediation server where compliance files are published from the core. The name of the Web share should be LDLogon. The path can be either a UNC path or mapped drive path (or local path). A UNC path is recommended (see the Important note above).
- **Browse:** Opens the local Windows Explorer window where you can navigate to the remediation server's LDLogon share.
- **User name:** Identifies a valid user with access credentials to the Web share on the remediation server.
- **Password:** Identifies the user password.
- **Confirm password:** Verifies the user password.
- **OK:** Saves the remediation server settings and adds it to the list in the Configure remediation servers dialog.
- **Cancel:** Closes the dialog without saving the settings and without adding it to the list of remediation server.

Next steps: Publishing remediation infrastructure files to remediation servers

The next step in setting up and configuring a remediation server is to publish or provision the remediation server with vital remediation infrastructure resources from the core server. These remediation infrastructure resources include:

- Security client (vulnerability scanner utility)
- Patches associated with the vulnerabilities contained in the Compliance group
- HTML pages that provide links to: install trust agents, perform compliance security scanning, and remediate detected vulnerabilities and other security exposures.

You must first define your compliance security criteria in the Security and Patch Manager tool before you can publish to servers.

For information about these tasks, see *Configuring compliance security and publishing trusted access settings*.

A LANDesk DHCP server is required for the LANDesk DHCP solution; but it is not required in a Cisco-based NAC implementation.

The LANDesk DHCP server provides a temporary IP address (a quarantine IP address) to requesting devices. With a temporary IP address, the device can communicate with the remediation server, which runs the security client (a special version of the security and patch scanner, or vulnerability scanner). The scanner scans for security definitions contained in the Compliance group, and if the vulnerability is detected, the remediation server will perform remediation by deploying the necessary patch files, or removing detected spyware, etc. Then, after remediation, the device requests an IP address again from the LANDesk DHCP server. If the device is healthy (according to the compliance rules), the LANDesk DHCP server forwards the device to the primary corporate DHCP server to be assigned a valid network IP address.

Important: Technical knowledge and expertise required for setting up LANDesk Trusted Access

Note that LANDesk Trusted Access requires additional hardware and software configuration beyond the basic LANDesk core server installation. Because of the technical nature of this additional set up work, this guide assumes you are familiar with either Cisco Network Access Control (NAC) and Cisco Secure Access Control Server (ACS) configuration and operation, and/or DHCP server management and DHCP protocols, as well as advanced networking infrastructure design principles and administration.

Read this chapter to learn about:

Setting up a LANDesk DHCP server

- LANDesk DHCP server prerequisites
- Determining server location on the network
- Installing the LANDesk DHCP plug-in on the primary DHCP server
- Installing the LANDesk DHCP server software
- Copying LANDesk certificate files to the LANDesk DHCP server
- Configuring the LANDesk DHCP server
- Using the LANDesk DHCP Manager tool to configure DHCP settings and create scopes
- Restarting the LANDesk DHCP server

LANDesk DHCP server prerequisites

You must make sure your network and router configuration meet the following conditions in order for LANDesk DHCP trusted access to work properly:

Network and router configuration requirements

- The LANDesk core server should not be visible to the quarantine network
- The router must be located between the LANDesk DHCP server and connecting devices
- The router must have DHCP forwarding turned on
- Add a VLAN subnet to the client interface on your router
- Change the IP address helper (relay agent) on the client interface to point to the LANDesk DHCP server instead of the primary DHCP server
- Add ACL rules on the router to restrict traffic from the VLAN so that devices can only reach the remediation server and subnet representatives

You should also make sure the server machine you want to set up as your LANDesk DHCP server meets the following requirements:

Special considerations and requirements for the LANDesk DHCP server

- The LANDesk DHCP server must be Windows 2000 or above, with .NET Framework 1.1
- The LANDesk DHCP server must be on the opposite side of the router from connecting devices
- The LANDesk DHCP server must have a static IP address (configured via Windows network configuration)
- The LANDesk DHCP server can't be a current DHCP server
- The LANDesk DHCP server can't be a PXE representative machine

Determining the server location on the network

As stated above, the LANDesk DHCP server must be on the opposite side of the router from the connecting devices, and on the same side of the router as the primary DHCP server.

You can see diagrams showing the component location and process workflow for each LANDesk Trusted Access solution in their respective overview sections. See, Using the LANDesk DHCP solution, and Using the Cisco NAC solution.

Installing the LANDesk DHCP plug-in on the primary DHCP server

The plug-in notifies the LANDesk DHCP server what IP addresses were handed out to the devices. The LANDesk DHCP server can then communicate with the device to ensure that the health state of the device has not changed. If the health state has changed, then the LANDesk DHCP server can force the device to renew its IP address and get a device address.

The steps below are for installing the LANDesk DHCP plug-in to the Microsoft DHCP server running on Windows 2000 server or 2003.

To install the LANDesk DHCP plug-in on the primary Microsoft DHCP server

1. Copy LDDHCPPlugin.dll and LDDHCPPlugin.reg from:
LDMain\Install\TrustedAccess\LDDHCP\MicrosoftDHCP on the core server to any local folder on your primary Microsoft DHCP server.

2. Edit the LDDHCPPlugin.reg file for the correct path and IP address to the LANDesk DHCP server.
3. Import the LDDHCPPlugin.reg file into the registry.
4. Restart the Microsoft DHCP service.

Plug-in for Linux DHCP servers

You can also install a LANDesk DHCP plug-in if you have a Linux DHCP server on your network. See the readme file (located in LDMain\Install\TrustedAccess\LDDHCP\Linux DHCP) for instructions on installing this plug-in.

Installing the LANDesk DHCP server software

To install and set up a LANDesk DHCP server

1. From the machine you want to set up as the LANDesk DHCP server, map a drive to your core server's LDMain\Install\TrustedAccess\LDDHCP folder.
2. Launch the LDDHCP.EXE install program.
3. Select the language version you want to install, and then click **OK**.
4. At the Welcome screen, click **Next**.
5. Accept the license agreement, and then click **Next**.
6. To copy the necessary files, click **Install**.
7. When the file copy process is complete, click **Finish**.

Note: The LANDesk DHCP server is not running yet. You must first configure LANDesk DHCP settings and click **Restart**.

Copying LANDesk certificate files to the LANDesk DHCP server

In order for the LANDesk DHCP Server to communicate with managed devices, you must copy your LANDesk certificate files to the LANDesk DHCP Server machine.

To copy the LANDesk certificate files,

1. From the LANDesk DHCP server machine, map a network drive to access the core server's administrative share. Use the following command syntax:
\\computername\c\$
(**Note:** You'll need administrator equivalent credentials in order to access this share on the core server.)
2. Copy the *.CRT and *.KEY files from the core server's C:\Program Files\LANDesk\Shared Files\keys folder to the same folder on the LANDesk DHCP server (this folder is automatically created by the installation program).

Configuring the LANDesk DHCP server

You've successfully installed the LANDesk DHCP server software. However, the LANDesk DHCP service is NOT yet running. The next step in setting up the LANDesk DHCP server and starting the service is to run the LANDesk DHCP Manager tool that has been installed on this machine by the setup program in order to configure DHCP server settings, configure posture validation server settings, create and manage scopes, and to add devices to the posture exclusion list.

Important note on opening firewall ports

Before you proceed in setting up the LANDesk DHCP server, you should disable the Windows Firewall if it is enabled. If you want to leave the Windows Firewall enabled, you must ensure the following UDP ports are completely open: 67, 68, 12576, and 12577.

Using the LANDesk DHCP Manager tool to configure settings and create scopes

The name of the LANDesk DHCP server configuration tool is LANDesk DHCP Manager. This tool can be launched either from the Start menu (**Start | Programs | LANDesk | LANDesk DHCP Server | LDDHCP Configuration**), or by double-clicking the **LDDHCP Configuration** icon that should now appear on the server's desktop.

The LANDesk DHCP Manager tool lets you:

- Configure LANDesk DHCP server settings
- Configure posture validation server settings
- Create and manage scopes (name, lease time, address range, relay address, exclusion range, and scope options)
- Add devices to the posture exclusion list
- Enable/disable the **Allow everyone access** setting (at the server level)
- Stop and restart the LANDesk DHCP service

To configure LANDesk DHCP server settings

1. At the LANDesk DHCP server you've installed, click the LANDesk DHCP Configuration program icon located on the desktop. (Or you can click **Start | Programs | LANDesk | LANDesk DHCP Server | LDDHCP Configuration**)
2. Right-click the **LANDesk DHCP server** object, and then click **Properties**. The **Configure LANDesk DHCP settings** dialog displays.
3. Enter the IP address of the LANDesk DHCP server. This field defaults to the IP address of the primary NIC in the server.
4. Enter the IP address of the primary DHCP server on your network.
5. Specify the frequency of the address pool backup (in minutes). This setting controls how often the LANDesk DHCP server saves IP address pool information. This information is saved in an XML file on the DHCP server.
6. Specify the minimum logging level by selecting an option from the drop-down list. Available logging levels include: Information, Warning, Error, Critical Error, and Debug. The different logging levels determine how much information is written to the log file.
7. If you want to allow all connecting devices to access the network (whether their posture status is determined to be healthy or unhealthy according to the compliance security criteria), click the **Allow access to everyone** checkbox. This setting is enforced at the DHCP server level and will apply to all scopes configured in the LANDesk DHCP server. Enabling this option forces all connecting devices to bypass the posture validation server process. (See note below.)

8. Click **OK** to save your settings and exit the Configure LANDesk DHCP settings dialog.

Using the Allow access to everyone option

You can use this option to allow time to finalize the configuration of your trusted access network and compliance security policy, to let the regular Security and Patch Management process bring the majority of your managed devices into compliance, to observe the various trusted access logs and reports, and to choose the right time to begin enforcing a compliance security policy and restricting network access. Once the majority of managed devices are compliant, or whenever you as the network administrator feels it is time, unchecking this option enables trusted access on your network and blocks network access to devices that are found to be non-compliant.

Once you've configured the basic settings for the LANDesk DHCP server, you can configure the posture validation server and create scopes.

About the Configure LANDesk DHCP settings dialog

Use this dialog to configure the basic LANDesk DHCP server settings:

- **LANDesk DHCP server:** Identifies the IP address of the LANDesk DHCP server you're configuring. This field defaults to the IP address of the primary NIC in the server.
- **Primary DHCP server:** Identifies the IP address of the primary (real) DHCP on your network. The LANDesk DHCP server communicates with the primary DHCP server in order to assign a permanent IP address to healthy connecting devices during the posture validation process.
- **Frequency of address pool backup (minutes):** Specifies how often the LANDesk DHCP server saves IP address pool information. This information is saved in an XML file on the DHCP server.
- **Minimum logging level:** Specifies how much information is written to the log file. Available logging levels include: Information, Warning, Error, Critical Error, and Debug.
- **Allow access to everyone:** Allows everyone access to the network, whether their posture is determined to be healthy or unhealthy. This option is checked by default. Use this option if you're using the LANDesk DHCP trusted access implementation and want to allow everyone access to the network. (See note above.)

To configure the posture validation server settings

1. In the LANDesk DHCP Manager tool, right-click the **Posture validation server** object, and then click **Properties**. The **Posture validation server** dialog displays.
2. Enter the IP address of the posture validation server. (**Note:** You should have only one posture validation server per LANDesk DHCP server.)
3. Enter the port number. The default port is: 12576.
4. Enter the URL to the Healthy status page. The name of this HTML files is: healthy.html. You should enter the full path to the file, including the http:// protocol identifier. This HTML page should have already been published from the core server to the remediation server, so typically the full path would be:
http://remediation servername/LDLogon/healthy.html.
(**Note:** This page informs the end user of a connecting device that their device has been scanned, passed the compliance security criteria, is considered healthy, and will be granted full access to the corporate network. The HTML pages are merely templates and can be edited to suit your specific trusted access security needs and requirements.)

5. Enter the URL to the Unhealthy status page. The name of this HTML file is: unhealthyLDDHCP.html. You should enter the full path to the file, including the http:// protocol identifier. As with the healthy status page, this HTML page should have already been published from the core server to the remediation server, and typically the full path would be:
http://remediation servername/LDLogon/unhealthyLDDHCP.html
(**Note:** This page informs the end user of the a connecting device that their device has been scanned and does not meet the compliance security credentials, is considered unhealthy, and has been denied access to the network. The page also provides links that lets the user either be granted Internet access only, or lets them download and install the necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network. The HTML pages are merely templates and can be edited to suit your specific trusted access security needs and requirements.)
6. Click **OK** to save your settings and exit the **Posture validation server** dialog.

About the Posture validation server dialog

Use this dialog to configure the posture validation server so that it can communicate with the LANDesk DHCP server, and so that the posture validation server knows where the healthy and unhealthy HTML pages are hosted on the remediation Web share to serve to connecting devices.

- **Posture validation server:** Identifies the IP address of a posture validation server.
(**Note:** You should have only one posture validation server per LANDesk DHCP server.)
- **Port:** Identifies the port on the posture validation server for communication with the DHCP server. The default port is: 12576.
- **Healthy URL:** Specifies the full path to the Healthy HTML page, including the http:// protocol identifier. This HTML page should have already been published from the core server to the remediation server, so typically the full path would be:
http://remediation servername/LDLogon/healthy.html.
(**Note:** This page informs the end user of a connecting device that their device has been scanned, passed the compliance security criteria, is considered healthy, and will be granted full access to the corporate network. The HTML pages are merely templates and can be edited to suit your specific trusted access security needs and requirements.)
- **Unhealthy URL:** Specifies the full path to Unhealthy HTML page. This HTML page file should have already been published from the core server to the remediation server, and typically the full path would be:
http://remediation servername/LDLogon/unhealthyLDDHCP.html
(**Note:** This page informs the end user of the a connecting device that their device has been scanned and does not meet the compliance security credentials, is considered unhealthy, and has been denied access to the network. The page also provides links that lets the user either be granted Internet access only, or lets them download and install the necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network. The HTML pages are merely templates and can be edited to suit your specific trusted access security needs and requirements.)

Using scopes

In order for the LANDesk DHCP server to lease temporary (or quarantine) IP addresses to connecting devices, you must first create and activate scopes. A scope is a range of possible IP addresses for a network or subnet.

Guidelines for creating scopes on your LANDesk DHCP server

- You should create a scope for each subnet (router) on your network
- Each scope should be configured with two gateways: one for a primary subnet and one for a quarantine subnet
- Each scope should have a unique relay server address (IP helper or relay agent)
- No two routers can have the same quarantine subnet IP range
- After you create a scope, you must configure the scope options (**Important:** option 001 and 003 are required)
- We recommend that you don't rename scopes after you've created them with the LANDesk DHCP manager tool.

To create and configure scopes

1. In the LANDesk DHCP Manager tool, right-click the **LANDesk DHCP server** object, and then click **New scope**. The **Scope properties** dialog displays. Or, to edit an existing scope, right-click the **scope** object in the LANDesk DHCP server tree, and then click **Properties**.
2. On the **Name** tab, enter a name and description for this scope. Each scope must have a unique name.
3. On the **Lease time** tab, enter a duration for IP addresses assigned to connecting devices by the LANDesk DHCP server. The duration should be equivalent to the amount of time a device is connected to the network.
4. On the **Address range** tab, enter a range of IP addresses (starting and ending IP addresses) that this scope can distribute to connecting devices. Make sure the range you specify provides enough IP addresses for the devices on your network.
(**Note:** You can't enter IP addresses that are part of the same subnet as the primary DHCP server's range.)
5. Also on the **Address range** tab, enter a subnet mask. You can enter either an IP address or a length. The subnet mask determines how many bits of an IP address to use for the network/subnet IDs, and how many bits of an IP address to use for the host IP.
6. On the **Relay address** tab, enter the IP address of the DHCP relay. Typically, this is the IP address on the router's client facing interface. The relay address determines which quarantine network/subnet from which to return IP addresses to connecting devices.
7. Click **Finish**.

Now you can configure the scope's options.

To configure scope options

1. Right-click the **Scope options** object under the scope you want to configure, and then click **Properties**.
2. You must configure at least the following scope option in order for the scope to work properly:
Option 003 (router gateway)
3. To configure an option, select it in the **Available options** list, fill in the required fields in the **Data entry** section below, check the option's checkbox to enable it, and then click **OK**.

About the Scope properties dialog

Use this dialog to create, configure, and modify scopes on the LANDesk DHCP server.

The **Scope properties** dialog contains the follows tabs:

About the Name tab

- **Name:** Identifies the scope (range of IP addresses for lease) on the DHCP server by a unique descriptive name.
- **Description:** Helps you remember the purpose of this scope.

About the Lease time tab

- **Lease time limited to:** Specifies the duration for IP addresses assigned to connecting devices by the LANDesk DHCP server. The duration should be equivalent to the amount of time a device is connected to the network.

About the Address range tab

- **Start IP address:** Identifies the first possible IP address in this scope's address range.
- **End IP address:** Identifies the last possible IP address in this scope's address range. Make sure the range you specify provides enough IP addresses for the devices on your network.
- **Subnet mask:** Identifies the subnet to which an IP address belongs.

About the Relay address tab

- **Relay address:** Specifies the IP address of the DHCP relay. Typically, this is the IP address on the router's client facing interface. The relay address determines which quarantine network/subnet from which to return IP addresses to connecting devices.

About the Subnet (Address pool properties) dialog

Use this dialog to modify a scope's IP address range or pool. You can access this dialog by right-clicking the **Address pool** object under the scope you want to modify, and then click **Properties**.

- **Start IP address:** Identifies the first possible IP address in this scope's address range.
- **End IP address:** Identifies the last possible IP address in this scope's address range. Make sure the range you specify provides enough IP addresses for the devices on your network.
- **Subnet mask:** Identifies the subnet to which an IP address belongs.

About the Exclusion range dialog

Use this dialog to configure and exclusion range. An exclusion range is a group of IP addresses that the DHCP server will not lease to devices. When creating a scope, you should determine whether any devices on your network, such as DNS servers, will need to use static IP addresses. If you have devices that need a static IP address, create an exclusion range so that you can assign all statically configured devices an IP address from the exclusion range.

To create a single IP address to exclude from the scope's lease pool, enter a starting IP address and leave the ending IP address field empty.

- **Start IP address:** Identifies the first possible IP address in this exclusion range.
- **End IP address:** Identifies the last possible IP address in this exclusion range.

About the Configure scope options dialog

Use this dialog to configure various scope options. Do not activate a scope until you specify the options you want. Scope options are inherited as default values for all devices in the applicable scope.

- **Available options:** Lists the scope options you can configure. Select the option you want to configure to display the data fields below.
- **Description:** Indicates the function of the selected scope option.
- **Data entry:** Specifies the information that must be filled in when configuring a scope option. This area displays when you select an option from the list of available scope options above. Fill in the fields, and then click **OK**.

Adding devices to the posture exclusion list

To add devices to the posture exclusion list

1. Right-click **MAC exclusions** object, and then click **Properties**.
2. Enter the MAC (machine) address of the device you want to bypass the posture validation process altogether, and then click **Add**.
3. You can enter as many device MAC addresses as you want.

About the MAC address exclusions dialog

Use this dialog to add devices that you want to bypass the posture validation process.

- **MAC address:** Indicates the machine address of the device you want to bypass the posturing process.
- **Add:** Adds the device to the list.
- **Remove:** Remove the device from the list.

Importing and exporting MAC address exclusions

To import address exclusions, right-click the **MAC Exclusions** object, click **Import**, and then browse to select the CSV file that contains the MAC addresses of devices you want to bypass the posture validation process.

To export address exclusions in your list, right-click the **MAC Exclusions** object, click **Export**, and then save the CSV file.

Restarting the LANDesk DHCP server

Any time you change LANDesk DHCP server settings, or scope settings, you must restart the LANDesk DHCP server in order for your changes to take affect.

You can restart the LANDesk DHCP server from the **File** menu, or by right-clicking the LANDesk DHCP server object and clicking **Restart**.

Once you've set up either a LANDesk DHCP or a Cisco NAC trusted access environment, the compliance security management tasks described below apply to both solutions.

Note: For either of the two trusted access solutions you should have already set up both a posture validation server and a remediation server and configured (or added) them in the console. For more information, see [Setting up and configuring a posture validation server](#), and [Setting up and configuring a remediation server](#).

Read this chapter to learn about:

Configuring compliance security and publishing trusted access settings

- Defining compliance security criteria in the Security and Patch Manager tool
- Defining healthy and unhealthy postures
- Publishing trusted access settings
- Configuring alternate user credentials
- Understanding the HTML pages

Other compliance security management tasks

To learn more about compliance scanning and other trusted access management tasks such as: updating compliance security rules and policies on posture validation servers, updating remediation resources on remediation servers, adding unmanaged devices to the Unmanaged Device Discovery tool, viewing affected devices, configuring logging, and generating reports, see [Managing compliance security](#).

Defining compliance security criteria in the Security and Patch Manager tool

Compliance security criteria is defined by two factors:

- The vulnerability definitions and other security type definitions you add to the **Compliance** group in the Security and Patch Manager tool in the console
- AND by how you define healthy and unhealthy device postures in the **Configure trusted access settings** dialog in the console.

See the appropriate steplists below for each of these tasks.

About Security Suite subscriptions

You must have a LANDesk Security Suite content subscription in order to download the various "types" of security content, such as application and operating system vulnerability definitions (and required patches), spyware definitions, blocked application definitions, virus definitions, system configuration security threat definitions, etc.

Without a Security Suite license (or a core server activated with a Security Suite license), you cannot access the LANDesk Security Suite services, and can't define compliance security using those security definitions.

Downloading security type definitions

Use the Security and Patch Manager tool to download different security type definitions, such as vulnerability, spyware, antivirus, and security threat definitions. This task is fully described in the Security and Patch Manager chapter. For more information on using the Security and Patch Manager download features, see Updating security and patch content.

Using the Compliance group to define a compliance security policy

As explained above, the contents of the Compliance group determine your compliance security policy. You can have minimal compliance security made up of just a few vulnerability and security threat definitions, or you can create a complex, strict security policy that is comprised of several security definitions. You can also modify the compliance security policy at any time simply by adding and removing definitions from the Compliance group.

Role-based administration right required to use the Compliance group

Only a LANDesk administrator or a user with the Security and Patch Compliance right can add or remove definitions to and from the Compliance group.

The following security content types can be added to the Compliance group to define a compliance security policy:

- Antivirus definitions
- Custom definitions
- Driver update definitions
- LANDesk software update definitions
- Security threat definitions (includes firewall definitions)
- Software update definitions
- Spyware definitions
- Vulnerability (OS and application) definitions

Note: You can't add blocked application definitions to the Compliance group to define compliance security policies.

To add security definitions to the Compliance group

1. In Security and Patch Manager, select the type of security content you want to add to your compliance security policy from the **Type** drop-down list, and then drag and drop definitions from the item list into the **Compliance** group.
2. Or, you can right-click an individual definition or selected group of definitions, and then click **Add to compliance group**.
3. Make sure any necessary associated patches are downloaded before you publish trusted access content to posture validation servers and remediation servers. You can right-click a definition, selected group of definitions, or the **Compliance** group itself, and then click **Download associated patches** to download the patches necessary to remediate affected devices.

Defining healthy and unhealthy postures

Your compliance security policy is also comprised of the healthy and unhealthy posture definitions you configure in the console.

To define healthy and unhealthy postures

1. **Prerequisite:** For the LANDesk DHCP solution, make sure you have already set up at least one posture validation server, remediation server, and LANDesk DHCP server. For the Cisco NAC solution, make sure you have already set up a Cisco router, Cisco Secure ACS, posture validation server (with connection to the Cisco Secure ACS), and a remediation server.
2. Make sure you've downloaded the security definitions (spyware, vulnerabilities, security threats, etc.) and patches you want to include in your security compliance policy using the Security and Patch Manager tool, and added those definitions to the **Compliance** group.
3. In Security and Patch Manager, right-click the **Trusted Access** group, and then click **Configure trusted access**.
4. To define the healthy posture (or status) for devices attempting to access the corporate network, select the number of hours since the last compliance security scan from the drop-down list. The default value is 96 hours.
(**Note:** This setting applies to both the LANDesk DHCP and Cisco NAC environments and posture validation processes.)
5. To define the unhealthy posture (or status), select the unhealthy posture from the drop-down list (possible unhealthy values include: Quarantine, Checkup, and Infected). These default postures should already be predefined in the Access Control Lists (ACLs) on the Cisco Secure ACS.
(**Note:** This setting actually applies only to Cisco NAC trusted access. With LANDesk DHCP trusted access, a device is either healthy or unhealthy based on the security definitions in the Compliance group and the healthy posture definition. If the device doesn't meet those conditions the device is unhealthy)

Publishing trusted access settings

Publishing trusted access settings sends information to posture validation servers and remediation servers that is required in order to implement the posture validation process and enforce compliance security. Publishing trusted access settings applies to both the LANDesk DHCP and the Cisco NAC solutions.

In order to publish trusted access settings from the console, you must have at least one posture validation server, one remediation server, and user credentials configured.

The initial publish must include All settings

The first time you publish trusted access settings to your posture validation servers and remediation servers, you must include ALL of the trusted access settings, including: trusted access content and infrastructure files (see below for details about these files). Subsequent publishing can include trusted access content or compliance rules only. Typically, the infrastructure files only need to be published once to remediation servers.

To publish trusted access settings

1. You can access the **Publish trusted access settings** dialog (and publish the settings) from several locations in the Security and Patch Manager tool. For example, you can right-click the Trusted Access object or the Compliance group, and then click **Publish**. You can also find the **Publish** button on the **Configure trusted access** and **Configure remediation server** dialogs. Additionally, you can click the **Publish trusted access settings** toolbar button in the Security and Patch Manager window.
2. To publish all of the trusted access settings, including the trusted access content and the Infrastructure files to all of your posture validation servers and remediation servers at once, select the **All** checkbox and click **OK**.

3. If you want to publish only the trusted access content (security definitions, trusted access settings or compliance rules, and associated patches) to posture validation servers and remediation servers, check the **Trusted access content** checkbox, and then click **OK**.
4. If you want to publish only the Infrastructure files (security client scanner, trust agent installs, and HTML pages) to remediation servers, check the **Infrastructure** checkbox, and then click **OK**. (Typically, you only have to publish the Infrastructure files only one time to remediation servers.)

About the Publish trusted access settings dialog

Use this dialog to publish trusted access settings to posture validation servers, and to publish remediation settings (resources) to remediation servers on your trusted access network.

- **All:** Published both trusted access content and Infrastructure files to the appropriate servers.
- **Trusted access content:** Publishes the trusted access content and settings you've defined in the Security and Patch Manager tool to all of the posture validation servers and remediation servers that have been added to your network.
Important: You must have at least one posture validation server on your network in order to publish trusted access content.
 - Trusted access content represents the vulnerability and other security content type definitions that currently reside in the **Compliance** group in the Security and Patch Manager tool, as well as the trusted access settings such as healthy and unhealthy posture settings, logging levels, etc. that are defined in the **Configure trusted access settings** dialog. Security definitions, healthy and unhealthy posture settings, and logging levels are published to posture validation servers, while associated patch files are published to remediation servers (based on the contents of the Compliance group at the time you publish).
(Note: If you change the contents of the **Compliance** group or change trusted access settings on the **Configure trusted access** dialog, you must republish this data to your servers.)
- **Infrastructure:** Publishes the following remediation resources to all of the remediation servers that have been added to your network.
 - **Setup and support files:** Setup and support files represent the security client scanner and trust agent installs. The security client scanner performs security scanning and remediation on devices. There are currently four versions of the security client: NAC, NAC for NT4 clients, DHCP, DHCP for NT4 clients. The security client scanner also includes a minimal LANDesk standard agent. Trust agent installs let end users install the LTA and CTA on their devices from a Web URL.
 - **HTML pages:** Represents the template HTML pages that are served by the remediation server to devices with trust agents installed that are trying to access your corporate network. These pages tell the end user what to do in order to gain limited access to the network, or to have their computers remediated in order to become compliant with your security policy and gain full access to the corporate network. These HTML pages are templates that you can modify.
(Note: Typically, the Infrastructure files only need to be published once to remediation servers. Unlike the trusted access content (compliance criteria), you don't need to republish these files every time you change the compliance security policy.)

Configuring alternate user credentials

If the connecting devices (attempting to access the network) are not logged in with local administrator rights, LANDesk Trusted Access uses this list of alternate user credentials to attempt to gain administrative rights to the device. Otherwise, the security client scanner cannot run and the user will need to log off and back on with administrative rights and try again (such as vendors or visitors). LANDesk Trusted Access will use these credentials to try to access the devices in order to scan for vulnerabilities and to deploy and install patches for remediation.

To configure alternate user credentials

1. In Security and Patch Manager, right-click the **Trusted Access** group, and then click **Configure credentials**.
2. Enter a user name for a user with administrative rights.
3. Enter the user password twice.
4. Click **Add** to add the user credentials to the list to the right
5. These user credentials will be used in the order they are listed if the end user of the connecting device is not logged in with administrative rights.

About the Configure credentials dialog

Use this dialog to identify alternate user credentials for access to end user devices for security scanning and remediation, in case the logged in end user doesn't have administrative access rights.

- **User name:** Enter a user name commonly used for an LANDesk Administrator user on your network.
- **Password:** Enter the password for that user.
- **Confirm password:** Re-enter the password.
- **Add:** Adds the user credentials in the list to the right.
- **Remove:** Removes the selected user from the User name list.
- **OK:** Saves your changes and exits the dialog.
- **Cancel:** Exits the dialog without saving your changes.

Understanding the HTML pages

The HTML pages are published to remediation servers with the Publish trusted access settings tool in the console. HTML pages are part of the remediation infrastructure files.

HTML pages are template files

The HTML pages are merely templates, and you should modify them to suit your own trusted access network needs and requirements.

After installing LANDesk Management Suite, these files are located in the following folder on the core server: ManagementSuite\Install\TrustedAccess\RemediationServer

Typically, these files only need to be published once to remediation servers.

The sections below describe the purpose of each HTML page.

Healthy status page

This HTML page should be used to inform the user of a connecting device that the device has been determined to be healthy, according to the compliance security credentials, and that it has been granted full access to the corporate network.

The name of this HTML page is: healthy.html

The healthy status page will ONLY be seen when a device transitions from unhealthy to healthy. It will not display each time a device postures as healthy.

The URL to this page on the remediation server should be entered in the **Healthy URL** field when you configure a posture validation server.

Unhealthy LANDesk DHCP page

This HTML page should be used to inform the user of a device attempting to access your network that the device has been scanned and does not meet the compliance security credentials, is considered unhealthy, and has been denied access to the network.

The name of this page is: unhealthyLDDHCP.html

This page provides links that lets the user either be granted Internet access only, or lets them download and install the trust agent and necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network.

The URL to this page on the remediation server should be entered in the **Unhealthy URL** field when you configure a posture validation server.

Unhealthy Cisco NAC page

This HTML page should be used to inform the user of a device attempting to access your network that the device has been scanned and does not meet the compliance security credentials, is considered unhealthy, and has been denied access to the network.

The name of this page is: unhealthyCisco.html

This page provides links that lets the user either be granted Internet access only, or lets them download and install the trust agent and necessary software for remediation so that their device can be repaired, rescanned, and allowed full access to the network.

The URL to this page on the remediation server should be entered in the **Unhealthy URL** field when you configure a posture validation server.

Once you've set up either a LANDesk DHCP or a Cisco NAC trusted access environment, the subsequent ongoing compliance security management tasks described in this chapter apply to both solutions.

Read this chapter to learn about:

Managing compliance security

- Ensuring trusted access services is enabled (turned on)
- Using the allow/restrict access to everyone option
- Understanding what happens when connecting devices are postured
- Viewing affected (non-compliant) devices

- Modifying and updating compliance security policies
- Adding unmanaged devices to the Unmanaged Device Discovery tool
- Configuring and viewing compliance logging
- Generating compliance reports

Ensuring trusted access services is enabled (turned on)

LANDesk Trusted Access services is essentially enabled (or turned on) when all of the following conditions exist:

- A **network control device** is set up and configured properly, with the necessary services running. For Cisco NAC, this is the router and the Cisco Secure ACS. For LANDesk DHCP, this is your network router/switch and the LANDesk DHCP server (with the plug-in to the primary DHCP server).
- The **Security and Patch Manager tool** can be accessed in the console by a user with the necessary rights, and a valid **Security Suite content subscription** allows you to download some or all security content types (definitions and required patches).
- At least **one security content definition** is contained in the Compliance group in the Security and Patch Manager tool. You can have as many definitions as you want to define your current compliance security policy depending on your security needs and goals, and the existing exposure risks. The contents of the Compliance group is the primary factor that defines your compliance security policy, and can include OS and application vulnerabilities, spyware, antivirus, software updates, custom definitions, and system configuration security threats including firewall configurations, whatever is critical in protecting your network at any given time. However, keep in mind that you must have at least one definition in the Compliance group in order for trusted access to be enforced and the posture validation process to occur. If the Compliance group is empty, there are no security credentials to check for, posture validation can't take place, and trusted access isn't operational.
- At least one **posture validation server** is set up and configured properly, with security compliance rules published to it from the core server (i.e., trusted access settings defining healthy and unhealthy postures, and Compliance group content information). In a Cisco NAC implementation, the posture validation server must be configured to communicate with the Cisco Secure ACS.
- At least one **remediation server** is set up and configured properly, with remediation resources published to it from the core server (i.e., the security client or vulnerability scanner utility, patches associated with the vulnerabilities contained in the Compliance group, and the HTML pages that provide links to: install trust agents, perform compliance security scanning, and remediate detected vulnerabilities and other problems).
- Make sure the **Allow access to everyone** option is disabled. In other words, with this option disabled, network access is determined by the health status of the connecting device as determined via the compliance policy and posture validation process. If you leave this option enabled, trusted access (the posture validation process) will in effect be turned off and any device, healthy or unhealthy, can access the network. See the section below for more information on using this option.

Establishing your own desired level of endpoint compliance security

If all of the conditions listed above are met, trusted access services IS running on your network.

Of course, there is flexibility built in to the service and you can customize how trusted access handles devices with options such as the Exclusion List and Allow Everyone On. You can also control the level of security by how many and exactly which security content definitions you place in the Compliance group, as well as the number of hours you specify before a compliance security scan runs automatically on connected devices.

By adjusting these options and policy criteria, you can define very strict, complex security policies or simple, lenient security policies, or any level in between. In other words, you have the ability to customize the degree of difficulty, or ease, with which a connecting device can comply with the security criteria you specify.

Most importantly, you can change the nature of your compliance security policy at any time in order to meet constantly changing circumstances and requirements. Just remember that any time you change your compliance security criteria (for example, the contents of the **Compliance** group in Security and Patch Manager, or the trusted access setting on the **Configure trusted access** dialog), you need to republish trusted access settings to your posture validation servers and remediation servers.

Using the allow/restrict access to everyone option

For both LANDesk Trusted Access solutions, you can literally turn on and off the entire posture validation process for your network with each solution's respective allow/restrict access option.

You can use this option to allow time to finalize the configuration of your trusted access network and compliance security policy, to let the regular Security and Patch Management process bring the majority of your managed devices into compliance, to observe the various trusted access logs and reports, and to choose the right time to begin enforcing a compliance security policy and restricting network access. Once the majority of managed devices are compliant, or whenever you as the network administrator feels it is time, enabling this option turns on trusted access on your network and blocks network access to devices that are found to be non-compliant.)

To allow access to everyone (disable the posture validation process)

If you leave this option enabled, trusted access (the posture validation process) will in effect be turned off and any device, healthy or unhealthy, can access the network.

For LANDesk DHCP

1. Open the LANDesk DHCP Configuration utility (on the LDDHCP Server)
2. Right-click the **LANDesk DHCP** server object, and then click **Allow everyone access**. This setting will apply to all scopes configured on the LANDesk DHCP server.
3. Healthy and unhealthy devices will be allowed on to your network until you change this setting.

For Cisco NAC

1. In Security and Patch Manager, right-click the **Trusted Access** group, and then click **Configure trusted access settings**.
2. At the bottom on the dialog, check the **Audit for reporting only** checkbox.
3. Healthy and unhealthy devices will be allowed on to your network until you change this setting.

Understanding what happens when connecting devices are postured

This section briefly describes the conditions when devices are checked for compliance via the posture validation process, and what happens when devices are postured.

Viewing posture validation process diagrams for both trusted access solutions

You can also view the posture validation process for devices with or without trust agents in both LANDesk Trusted Access environments. See the following two sections for the diagrams:

- Understanding the LANDesk DHCP components and process workflow
- Understanding the Cisco NAC components and process workflow.

In a LANDesk DHCP trusted access environment

A connecting device is forced to posture when:

- Acquiring an IP address
- Changing its IP address (release/renew)
- Renewing its IP address

When a connecting device without the LTA installed is postured:

- The device is placed in the quarantine network without warning or notification.
- The device may have limited network resources provided to it in the quarantine network
- A clientless status event is logged in the log file reports

When a connecting device with the LTA installed is postured and found to be unhealthy or non-compliant:

- The device is automatically presented with the Unhealthy URL
- A unhealthy status event is logged in the log file reports
- The end user can click the appropriate link to scan the device (NT4 machines use a different link)
 - The device is scanned and remediated if necessary
 - The Healthy URL is presented
 - A healthy status event is logged in the log file reports
 - The healthy devices is allowed access to the network
- Or, the end user can choose to browse the Web without having to scan (if the network administrator has set this up)

When a connecting device with the LTA installed is posture and found to be healthy or compliant:

- The device is allowed onto the network with no interruption
- A healthy status event is logged in the log file reports

In a Cisco NAC trusted access environment

A connecting device is forced to posture when:

- Attempting to connect to a network segment protected by Cisco NAC
- Periodically on a configurable interval

When a connecting device without the CTA installed is postured:

- The device is handled as clientless, and follows whatever rules have been set up for a clientless user in the Cisco Secure ACS

When a connecting device with the CTA installed is postured and found to be unhealthy or non-compliant:

- The device is presented with a message box (health statement), which can be set up in ACS to give instructions on what to do next for remediation
- A status is logged in the ACS log file (Healthy, Infected, Checkup, Quarantine, and Unknown)
- The end user must manually browse to the remediation page. Ideally the Cisco ACS message box (health statement) should be configured to display the URL
 - The end user can click the appropriate link to scan the device (NT4 machines use different link)
 - The device is scanned and remediated
 - The Healthy URL is presented
 - A healthy status event is logged
 - The device is allowed access to the network
- Or, the end user can choose to browse the Web without having to scan

When a connecting device with the CTA installed is posture and found to be healthy or compliant:

- The device is allowed onto the network with no interruption
- A healthy status event is logged

Viewing affected (non-compliant) devices

When you want to see which devices have been postured and are found to be unhealthy or non-compliant,

1. In the Security and Patch Manager tool, click the **Computers out of compliance** toolbar button.
2. Or, right-click the **Compliance** group, and then click **Affected computers**.
3. A dialog displays that lists non-compliant devices.
4. You can select a device in the list to view the security definitions (in a list below) with which the device is vulnerable or out of compliance.

Modifying and updating compliance security policies

You can modify and update your compliance security policy at any time.

You do this by changing the content of the **Compliance** group in Security and Patch Manager, and by changing trusted access settings such as the definitions of healthy and unhealthy postures and logging level in the **Configure trusted access settings** dialog in the console.

You then must republish the trusted access content to posture validation servers and remediation servers. Remember that publishing trusted access content sends trusted access settings and compliance rules to posture validation servers AND any associated patches to remediation servers; while publishing Infrastructure files sends setup and support files (including the security client scanner, trust agent installs, and HTML template pages) to remediation servers. (**Note:** Typically, the Infrastructure files only need to be published once to remediation servers. Unlike the trusted access content, you don't need to republish these files every time you change the compliance security policy.)

For detailed information, see Defining compliance security criteria in the Security and Patch Manager tool.

Adding unmanaged devices to the Unmanaged Device Discovery tool

If you want to add unmanaged devices in to the Unmanaged Device Discovery tool, so that they can be configured with LANDesk agents and scanned and remediated for compliance, follow the procedure below.

1. In Security and Patch Manager, right-click the **Trusted Access** group, and then click **Add unmanaged devices**. (**Note:** In order to add unmanaged devices you must have at least one posture validation server set up and configured in the console.)
2. Click **Tools | Configuration | Unmanaged Device Discovery** to open the tool, and then click the **Computers** group. You might need to refresh to see the newly added devices.

Configuring and viewing compliance logging

LANDesk Trusted Access provides the ability to configure and generate several log files for various posture validation processes. You can customize the logging levels (the amount of information written to the log files) for these logs. The log files are useful if you need to analyze certain processes or for troubleshooting.

About the posture validation server log

This log file is located on the posture validation server, at:
C:\Program Files\LANDesk\PostureServer\PostureServer.log

The posture validation server log shows

- All logged posture events (Healthy, Unhealthy, Unknown)
- Reasons for Unhealthy and Unknown events

To configure the logging level for posture validation server logs

1. In Security and Patch Manager, right-click the **Trusted Access** group, and then click **Configure trusted access**.
2. Select a **Minimum logging level** from the drop-down list. Available logging levels include: Information, Warning, Error, Critical Error, and Debug.
3. The logging level you specify applies to all posture validation servers in the list.

To view posture validation server logs

You can view the log file directly at the posture validation server at the path noted above.

Or, a more convenient access to the posture validation server logs is from the console's Security and Patch Manager tool. Simply open the **Trusted Access** object in the Security and Patch Manager tree, and double-click the log file you want to view online.

About the LANDesk DHCP service log

Of course, this log file applies only to the LANDesk DHCP solution.

This log file is located on the LANDesk DHCP server, at
C:\Program Files\LANDesk\LDDHCP\DHCPService.log

The LANDesk DHCP service log shows:

- All logged DHCP events from the LDDHCP service
- Posture status of devices requesting DHCP leased IP addresses

You can configure the logging level for LANDesk DHCP logs in the LDDHCPSettings.xml file.

About the Cisco ACS log

Of course, this log file applies only to the Cisco NAC solution.

This log file is located on the Cisco Secure ACS machine. You can access this log file from the Cisco Secure ACS utility, under **Failed Authentications Log**.

Generating compliance reports

LANDesk Trusted Access is represented by several new trusted access and compliance related reports in the Reports tool. These reports provide a variety of useful information about trusted access attempts, unmanaged device discovery, healthy and unhealthy devices postures, compliance trends, compliance security policy, and compliance status for your trusted access network. Data for the trusted access and compliance reports comes from the server log files (mentioned above).

For example, some of the trusted access and compliance reports include:

- **All Log Entries**
- **Device/User Log Entries**
- **Devices Discovered**
- **Healthy Log Entries**
- **Summary**
- **Unhealthy Log Entries**

In order to access the Reports tool, and generate and view reports, a LANDesk user must have either the LANDesk Administrator right (implying full rights) or the specific Reports right.

LANDesk Trusted Access reports follow the same rules as the reports in the Software License Monitoring group, including their ability to be copied, removed, exported, and so on from the My Reports and User Reports groups.

Running and publishing reports

You can run any report from the Reports window. From the Reports window, right-click the report you want to run, and then click **Run** (or, click the **Run** toolbar button). The report data displays in the Report View.

You can also publish reports to a secure file share where they can viewed by any user you've given the proper access credentials.

For more information about using the Reports tool, and a complete listing of the trusted access and compliance reports (with descriptions), see Managing Reports.

Using connection control manager

Connection control manager monitors and restricts I/O devices and network connections. You can restrict the network IP addresses that devices are allowed to connect with, and you can also restrict the use of devices that allow data access to the device, such as ports, modems, drives, and wireless connections.

For connection control manager to function on a device, you must have the local scheduler agent and the standard LANDesk agent deployed on that device. Every time the device initiates a network/device connection or makes changes to a network/device connection, the connection control manager agent applies configuration rules. These rules include terminating connections that aren't allowed and sending alerts to the core server.

Use **Connection control configurations** to manage network connections. You can configure network restrictions in two general ways: by specifying which network addresses are allowed or by specifying which network addresses are blocked.

Use **Device control configurations** to manage USB, PCMCIA, and Bluetooth connections. You can configure USB restrictions by either generically blocking a whole class of USB devices, such as storage devices, or by using advanced settings to restrict certain USB devices based on information you specify.

Each connection control configuration that you define is saved and can be applied to the managed devices that you specify. You can save multiple configurations and apply them to different devices as needed. When you create a configuration, you must deploy it to devices for it to take effect. Connection control manager supports devices running Windows 2000, Windows Server 2003, and Windows XP.

Note: Connection control manager is part of LANDesk Security Suite. Connection control manager isn't available unless you have a Security Suite license.

Read this chapter to learn about:

- Using connection control configurations to restrict network access
- Using device control configurations to restrict USB device access
- Configuring advanced USB settings
- Deploying configurations

Using connection control configurations to restrict network access

Use the connection control configurations to help limit network access to authorized networks or IP addresses, or block communication with specific networks.

You can define either inclusive or exclusive network restriction rules:

- An inclusive rule specifies only the network addresses that **are** allowed (**Limit connections to listed networks**); anything not within the specified IP address ranges is not allowed.
- An exclusive rule specifies the network addresses that **aren't** allowed (**Block connections to listed networks**); all network connections are allowed except for those that are specifically excluded.

For example, to maintain a “clean network” environment for a device, you would select **Limit connections to listed networks** and enter the range of IP addresses that are allowed. Attempts to access any other IP address from the device are blocked.

Another example is to allow access to any IP addresses except a range of restricted addresses (such as for a restricted corporate network). For this situation, select **Block connections to listed networks** and specify the range of IP addresses that can't be accessed.

To create a connection control configuration

1. Click **Tools | Security | Connection control manager**.
2. In the lower pane, click **Connection control configuration**.
3. Enter a **Configuration name**.
4. Check **Limit connections to listed networks** and list the network addresses that are allowed. If devices can be connected to other networks when not connected to restricted network addresses, check **Allow unlisted networks if not connected**.

OR

Check **Block connections to listed networks** and list the network addresses that aren't allowed.

5. Enter a range of IP addresses and click **Add**. Repeat as needed. To remove a range of IP addresses, select it from list and click **Remove**.
6. To verify that a core server is running on the network that the device is connecting to, check **Verify core server existence on the network**. This option applies only if **Limit connections to listed networks** was selected.

A range of IP addresses can sometimes be used by more than one network. For added security in restricting network access, you can ensure that the core server is running on a network before a device is allowed to connect to that network.

Check the **Verify core server existence on the network** box to implement this added security. If no core server is found on the network being accessed, the connection will be disabled.

Leave this check box clear if you're confident that the network addresses in the access list are trusted, or if you prefer to reduce traffic on the network by not sending pings to the core server.

About the Connection control configuration dialog

The Connection control configuration dialog has these options:

- **Configuration name:** The name for this configuration. This name appears in the main connection control manager window.
- **Limit connections to listed networks:** Only allows connections to the listed IP address ranges.
 - **Allow unlisted networks if not connected:** Allows connections to unlisted networks, but only if the device isn't already connected to a listed network.
- **Block connections to listed networks:** Blocks connections to the listed IP address ranges.
- **Starting IP address:** The starting IP address for the range you want to control.
- **Ending IP address:** The ending IP address for the range you want to control.
- **Add:** Adds valid IP address ranges to the controlled list.
- **Remove:** Removes the selected IP address range from the controlled list.
- **Verify core server existence on the network:** A range of IP addresses can sometimes be used by more than one network. For added security in restricting network access, you can ensure that the core server is running on a network before a device is allowed to connect to that network. Check this box to implement this added security. If no core server is found on the network being accessed, the connection will be disabled.

Allowing unlisted networks if not connected

Check the **Allow unlisted networks if not connected** box if you allow a device (such as a laptop) to connect to an unlisted network while it isn't connected to a network on the restricted list. Connection control manager ensures that the device connects only to listed networks or only to unlisted networks, but does not connect to both at the same time. After the device has connected to an unlisted network, the core server is notified that a connection was made outside of the listed IP addresses.

When the device is not connected to a network and then attempts to connect to unlisted IP addresses, it is allowed to connect and an alert is queued. The next time the device is connected to the network where the core server is running, the alert is sent from the device to the core server to notify the core server that a connection was made outside of the listed IP addresses.

If this box isn't checked, the device can connect only to listed network addresses.

Using device control configurations to restrict USB device access

Connection control manager configurations can have two parts. The first part is the connection control configuration, where you limit network access. The secondary part, a device control configuration, is optional. The device control configuration service, `usbmon`, runs on managed devices, where it monitors and restricts USB connections. The configurations are standalone, and you can deploy a device control configuration without deploying a connection control configuration.

By default, device control configurations can restrict the following types of devices. You can use the advanced USB settings to restrict any USB device or class of devices that you specify.

- Pocket PCs*
- Storage
- Keyboard and mice
- Printers
- Scanners
- Network volumes
- Bluetooth* Personal Area Networks
- PCMCIA* devices
- Palm* devices

The `usbmon` service can:

- Prevent the use of unauthorized USB and PCMCIA devices.
- Prevent the use of unauthorized removable storage devices.
- Trigger an external program or script when it detects an unauthorized device.

To create a device control configuration

1. Click **Tools | Security | Connection control manager**.
2. In the lower pane, click **Device control configuration**.
3. Enter a **Configuration name**.
4. Select whether you want the profile to apply to the current **User** or all users on the **Computer**. For more information, see Understanding profiles.
5. Select whether you want this profile to **Merge** with or **Replace** an existing profile.
6. Customize the options you want. For more information, see the next section.
7. Click **Create** to save your profile.

Connection control manager stores device control configurations in the core server's `LDLogon\usbmon` folder. Device control configurations are .INI files named with the configuration name you specified.

About the Device control configuration dialog

The **Device control configuration** dialog has these options:

- **Configuration name:** The name for this configuration. This name appears in the main connection control manager window.

- **Apply configuration to:**
 - **User:** Applies the configuration only to the user logged on at the time of deployment. For more information, see Understanding profiles.
 - **Computer:** Applies the configuration to all users on the device. For more information, see Understanding profiles.
- **Block USB devices, allow the following:**
 - **Keyboard and mice:** Checking this allows USB keyboards and mice, and adds Service=hidusb to the USB rules list. For more information on the rules list, see Configuring advanced USB settings.
 - **Pocket PC's:** Checking this allows devices to sync with Pocket PC handhelds, and adds Service=wceusbsh to the USB rules list.
 - **Storage:** Checking this allows USB storage devices, and adds Service=usbstor to the USB rules list.
 - **Printers:** Checking this allows USB printers, and adds Service=usbprint to the USB rules list.
 - **Palm devices:** Checking this allows devices to sync with Palm handhelds, and adds Service=PalmUSBD to the USB rules list.
 - **Scanners:** Checking this allows USB scanners, and adds Service=usbscan to the USB rules list.
- **Notify user when unauthorized USB devices are detected:** Checking this displays a message box when a user connects an unauthorized USB device. For more information, see Creating custom messages.
- **Advanced USB settings:** Displays the Device control advanced settings dialog, where you can see blocked devices and create your own rules to unblock devices. For more information, see Configuring advanced USB settings.
- **Block all unknown volumes:** Blocks access to any volume that wasn't present when the device control configuration was installed. Note that if a device containing a volume was attached when the configuration was installed, the usbmon service will allow that device in the future, even though it may be removable.
- **Notify user when unauthorized volumes are detected:** Checking this displays a message box when the usbmon service detects an unauthorized storage volume. For more information, see Creating custom messages.
- **Block Bluetooth Personal Area Networks (PAN):** Blocks access to Bluetooth networks.
- **Block PCMCIA devices, allow the following:**
 - **Network cards:** Checking this allows PCMCIA network cards.
 - **Storage:** Checking this allows PCMCIA storage cards.
- **Commands:** Allows you to configure commands that run when an unauthorized device is detected. For more information, see Configuring commands that run when an unauthorized device is detected.

Understanding profiles

The Device control configuration dialog has **Apply configuration to** and **Deployment options**. These options interact, and it's important to understand what is happening when you select each option. The table below describes the option interactions:

	User	Computer
Merge	The current configuration will be applied to the logged on user. All previous configurations to other users and the device will stay the same. The logged in user will get the current configuration.	All users without a private user configuration will get this current configuration. If a particular user already had a configuration, the previous configuration stays active.

Unauthorized device handling

Device control configurations use the usbmon service on managed devices. When the usbmon service receives notification from the OS that a new USB or PCMCIA device has been inserted, the usbmon service applies a number of custom defined rules to decide whether or not the device is allowed. You can set up simple rules to allow only certain types of devices such as keyboards and mice, printers, and scanners. More complex rules might allow only secure storage devices of a given manufacturer, or exclude devices of a given manufacturer.

When an unauthorized device is detected, the usbmon service will:

- Remove the device from the Windows Device Manager so Windows won't see it any more. Any drivers for the device remain installed.
- In the case of an unauthorized USB device or volume, optionally display a configurable message to the user (see Custom messages).
- Optionally load an external program (For more information, see Configuring commands). For example, the external program can be a script that sends an alert to a central console.
- Send a "Disabled device activated" AMS alert to the core server. The alert message includes the device name.

Removable storage device handling

Usbmon is the service on managed devices that restricts USB connections. When a new volume is mounted, the usbmon service receives notification from the operating system. The usbmon service then uses the GetDriveType() API call to check the type of drive that was mounted. If the OS describes the drive as "removable" or "fixed drive", the usbmon service will take action. The usbmon service also checks for removable volumes at boot time. If an unauthorized volume is found at boot time, the same actions are taken as when the volume is mounted later.

Drives that are considered removable include (but are not limited to) USB storage devices. CD drives (read-only or read/write) are not considered removable storage.

The OS doesn't consider hard drives as removable. The GetDriveType() call describes them as "fixed drive" even if they are attached via USB or some other external port. To allow removable hard drives to be handled the same as other removable storage devices, the usbmon service records the list of hard drives at the time the service is installed. For example, if a device has two hard drives (C: and D:) at the time the usbmon service is installed, the usbmon service will consider those drives as fixed and will not check them. But if at some later time a hard drive with drive letter E: is found, the usbmon service will consider it a removable device.

The usbmon service keeps the list of "fixed drives" in the registry at HKLM\Software\LANDesk\usbmon\FixedDrives. This list is created at the time the service is installed. The **Block all unknown volumes** option blocks access to any volume that wasn't present when the device control configuration was installed. Note that if a device containing a volume was attached when the configuration was installed, the usbmon service will allow that device in the future, even though it may be removable.

When a removable storage device is detected, the usbmon service will:

- Lock the volume. Users who attempt to access the volume will get an "access denied" error.
- Optionally display a configurable message to the user.
- Optionally load an external program. For example, the external program can be a script that sends an alert to a central console.

- Send a "Disabled device activated" AMS alert to the core server. The alert says a volume was activated, but additional information about the volume isn't available.

What if a support person needs to use a USB memory stick?

If you are an IT support person and you want to use a USB storage device on a user's computer, there are several things you can do:

1. Log on with admin rights and temporarily disable the usbmon service.
2. Log on with admin rights, run the usbmon GUI and add the device to the list of authorized volumes.
3. Use profiles. A device that is not allowed for the end user might be allowed when you log in on the same computer with your support account because you have a different usbmon profile.

Configuring advanced USB settings

Once connection control manager is installed on a device, the agent stores information about the last ten USB devices that it blocked access to. The inventory scanner sends this information to the core database. Information about these blocked devices then appears in the **Advanced USB settings** dialog. You can use this information to create advanced rules that allow or block specific USB devices. These advanced rules allow you to control more than just the basic device categories you see in the **Device control configuration** dialog.

In the **Advanced USB settings** dialog, you can base a rule on any of the six columns. Right-click on a value in the column and click **Allow** to create a rule that allows devices based on that attribute. The keywords created for each of the columns are the following:

```
DeviceDesc
HardwareID
Service
Mfg
LocationInformation
Class
```

These are the same names that are used in the registry under the HKLM\System\CurrentControlSet\Enum\USB key.

The most useful field to base rules on is usually **Service**. This corresponds to a Windows driver. For example, the driver for USB ActiveSync connections to Windows CE PDAs is called wceusbsh (see HKLM\CurrentControlSet\Services\wceusbsh). Any of the six columns can be used to base a rule on, however. It is up to you to decide which rules make sense for your situation.

Wildcards

You can use wildcards in rules, for example, the following would allow any device that has the string "floppy" in its device description:

```
DeviceDesc=*floppy*
```

Whitelist vs. Blacklist rules

All the rules illustrated so far have been whitelist rules, where devices are forbidden unless they satisfy at least one of the rules. The usbmon service also supports blacklist rules. Rules prefixed by a minus sign are blacklist rules. For example:

```
Service=usbstor
-DeviceDesc=*floppy*
```

The first rule allows USB storage devices. The second rule blacklists devices that have the string "floppy" in their device description.

If both whitelist and blacklist rules are defined, the usbmon service first checks devices against the whitelist rules. If there are no whitelist rules that allow the device, the device is forbidden. If there is at least one whitelist rule that allows the device, then the usbmon service checks the device against the blacklist rules. If the device satisfies none of the blacklist rules, it is allowed. Otherwise it is forbidden.

If only whitelist rules exist, a device is forbidden unless it satisfies one of the whitelist rules. If only blacklist rules exist, a device is allowed unless it satisfies one of the blacklist rules.

Composite rules

All the rules illustrated so far have been simple rules, where a single field is tested. Usbmon also supports composite rules, as in the following example:

```
Service=wceusbsh, DeviceDesc=*iPAQ*
```

This rule allows only Windows CE devices that have the string IPAQ in their device description.

Composite blacklist rules are also possible. Example:

```
Service=wceusbsh
-Service=wceusbsh, Mfg=*iPAQ*
```

The above two lines allow Windows CE devices, except those that have the string IPAQ in their manufacturer field. The above lines are equivalent to the following single line:

```
Service=wceusbsh, -Mfg=*iPAQ*
```

Creating custom messages when unauthorized devices/volumes are detected

In the **Device control configuration** dialog, you can customize the message text that the user sees when unauthorized devices/volumes are detected. In the message text, you can use these placeholders to show information about the unauthorized volume or device:

- %vol%: volume serial number
- %desc%: description
- %service%: service
- %hwid%: hardware ID
- %mfg%: manufacturer
- %loc%: location
- %class%: class

Configuring commands that run when an unauthorized device is detected

When the usbmon service detects an unauthorized volume or device, it can execute external programs. You can include one or two placeholders in the commands:

- %1: will be replaced with either "volume" or "device", depending on whether an unauthorized volume or an unauthorized USB device was detected.
- %2: will be replaced with either the volume serial number of the unauthorized volume, or with the identification string of an unauthorized USB device.

For example, a line such as the following:

```
wscript myscript.vbs %1 %2
```

might cause the following command to be launched:

```
wscript myscript.vbs volume "1234ABCD"  
wscript myscript.vbs device "Y-E Data USB Floppy: Vid_057b&Pid_0000"
```

Usbmon guarantees that only one instance of the script will be running at the same time.

To configure commands

1. In a device control configuration, click **Commands**.
2. Enter the commands you want.
3. Click **OK**.

Configuring alerts

Connection control manager configurations use the alert management system for alerting (**Tools | Alert settings | Connection control manager**). For more information on alerting, see Using alerts. Connection control manager can trigger alerts on these events:

- Configuration error
- Disabled device activated
- Restricted network connection attempted
- Unlisted network connection attempted
- Unlisted network session detected

Viewing the unauthorized device list

On each computer, connection control manager stores a list of the ten most recent unauthorized devices that were connected. You can view this information from the **Network view** by clicking **Inventory** on a device's shortcut menu. Then click **LANDesk Management | Connection control manager | Usbmon alert**.

Deploying configurations

Once you've created a connection control configuration or a device control configuration, you must deploy it to managed devices before it will be active.

To deploy a configuration

1. From the saved configuration's shortcut menu, click **Schedule**.
2. The configuration is added to the **Scheduled tasks** window. In this window, drag devices onto the configuration icon.
3. When all devices have been added, from the task's shortcut menu, click **Properties**. In the tree click **Schedule task**, and configure the scheduling options.

For more information on scheduling tasks, see Using scripts and tasks.

When you schedule a device control configuration for deployment, connection control manager does the following:

- It creates an executable distribution package that's named after the source device control configuration. The package's primary file is `usbmon.exe`. Additional files are `usbmon.reg`, `devactalert.exe`, `netres.mrl`, and `<device control configuration name>.ini`.
- If you target users for the device control configuration task, connection control manager uses a public policy-based delivery method called "Usbmon Pull Delivery." If this delivery method doesn't exist, connection control manager creates it. When task targets are users, connection control manager has to use a policy-based delivery method to ensure that the correct user gets the configuration. When target users log on, the policy-based delivery method activates and installs the configuration.
- If you target computers for the device control configuration task, connection control manager uses a public policy-supported push delivery method called "Usbmon Push Delivery." If this delivery method doesn't exist, connection control manager creates it. Since the configuration targets a device, any user that logs into that device will get that device control configuration; it doesn't matter who is logged in when the configuration gets installed. You can use push or policy delivery methods for computers.

Once connection control manager creates the `usbmon` policy or policy-supported push delivery methods, you can customize them. As long as the method name doesn't change, connection control manager will use the modified delivery method.

For more information on creating device control configurations locally on managed computers and deploying those configurations manually, view the `usbmon` help file, `usbmon.chm` in the core server's LDMain share.

Troubleshooting

- Each new connection control configuration is saved as a configuration file and a script file in the following folders:

```
ldmain\ccmgr\name.cfg
ldmain\scripts\name.ini
```

- If a script or configuration already exists with the same name that you give a configuration, you'll be prompted to overwrite the existing script or configuration. This can cause an unrelated distribution script of the same name to be overwritten.

- When entering IP ranges for network restrictions, don't restrict access to the network range the core server is on. If clients access a restricted network and connection control manager disables network access, only communication with the core server can restore network access. If devices can't communicate with the core server because of a restriction, network access can't be restored.
- When restricting access to I/O devices, don't restrict I/O devices that host network adapters. If you restrict access to I/O devices that host a network adapter, that client will no longer be able to access the network. For example, restricting USB access prevents any USB network adapters from working. Without network access, you won't be able to update restriction settings for that client.
- If you select the following options in connection control manager, and the core server isn't available on a listed network, clients will have unrestricted I/O device access while on that network.
 - Limit connections to listed networks
 - Allow unlisted networks if not connected
 - Verify core server existence on the network

If "Allow unlisted networks if not connected" is checked, and the agent can't find the core on a listed network, it will assume that the network is unlisted. At this point, unintended access may be granted to local I/O devices. This can create a security risk. Make sure the core server is available to prevent this from happening.

Using alerts

The LANDesk Alert Management System (AMS) automates actions in response to alerts that occur on the network. AMS monitors Management Suite components and devices for specific events to occur. When these events occur, the component or device sends an alert to AMS.

AMS can then notify you about the alert by completing the predefined alert actions you've configured. For example, you can configure the console to notify you if someone attempts a remote control session. When this event occurs, AMS detects the attempt and runs the configured alert actions such as sending you Internet mail or a pager message.

Read this chapter to learn about:

- How alerting works
- Configuring AMS alert actions
- Configuring the Message Box alert action
- Configuring the Broadcast alert action
- Configuring the Send Internet Mail alert action
- Configuring the Run Program alert action
- Configuring the Write to Event Log alert action
- Configuring the Load an NLM alert action
- Configuring the Send Page alert action
- Configuring the Send SNMP Trap alert action
- Working with configured alert actions
- Viewing the AMS Alert History

How alerting works

You can configure AMS to notify you when specific events occur. For example, you could configure a message box alert action to display at your device when a remote control session begins at a device. At the beginning of a remote control session, AMS would generate an alert and display the message box on your device. The console lets you configure alerts on certain parameters.

When the alert conditions you set occur, the console sends an alert to AMS. AMS notifies you by running the alert actions you have configured in the Alert Settings dialog. Available alert actions include:

- Displaying a message box
- Broadcasting messages
- Sending Internet e-mail
- Loading an NLM
- Running a program
- Writing the event details to an event log
- Sending a pager message
- Sending an SNMP trap

You can configure alerts for NetWare and Windows 95/98/NT/2000/2003 and Windows XP Professional devices. You can also select the device where the alert action occurs.

The alert actions you configure at one console aren't available at another. You can export configured alerts to other consoles to use the same configured alert actions on multiple devices. See "Exporting alert actions to other computers" later in this chapter for more information.

Configuring AMS alert actions

The **Alert settings** dialog is where you select alerts and configure alert actions. The **Alert settings** dialog contains a folder tree view of all events that AMS can monitor. You can expand or contract the folders to see the alerts available for each. You can also configure alert actions to occur when AMS detects any of these events.

Configuring alert action messages

These alert actions can generate messages when they are sent:

- Message box
- Broadcast
- Send page
- Send internet mail
- Send SNMP trap
- Write to event log

This message can include any text you add and information from the alert that generated the message. This table lists the default parameters available with all messages:

Default parameter	Description
Host Name	Name of the host device
Date	Date the alert occurred
Time	Time the alert occurred
Alert Name	Name of the selected alert
User Name	Name of the user who triggered the alert (if available)
Description	A description of the alert that occurred
Severity	The severity level of the alert

More parameters may be available depending on the selected alert. The Message dialog contains two list boxes. The Message box contains the text of the message you want to send. The Alert Parameters list contains any parameters you want included as message text.

Each parameter placeholder you add to the Message box is substituted with corresponding alert information when the alert occurs. Alerts can't be larger than 1 KB in size. When an alert is larger than 1 KB, it can't be delivered. In this case, AMS triggers a default alert to notify you that a message wasn't sent. You can configure alert actions for the default alert to ensure that you know when a message isn't delivered.

You can test configured alert actions to make sure they work as expected. See "Testing configured alert actions" later in this chapter for more information.

Configuring alert actions

You use similar steps to configure most AMS alert actions in the Configure Alerts wizard. For specific details about configuring each type of alert action, refer to that section later in this chapter.

To configure an alert action

1. In the console, click **Configure | Alert settings**.
2. In the **Alert settings** window, select the **alert** you want to configure alert actions for.
3. Right-click the **alert**, then click **Configure**.
4. Select an **alert action**, then click **Next**.
5. Select a **client** to run the action, then click **Next**.
6. Select an **alert action severity**, or use the default. You rate configured alerts so that an important alert can be flagged as critical. You can set other alerts that aren't as important to you at informational or monitor levels. AMS has six severity levels:
 - Monitor
 - Information
 - OK
 - Critical
 - Non-Critical
 - Non-Recover
7. Click **Next**.
8. Select **details** for the selected alert action, then click **Next**.
9. If the alert action can send message text, enter the **message text** you want to display in the Message box and move available parameters you want to use to the Message box.
10. Enter a **configuration name**. This name and the action computer name appear in the Alert Settings dialog beside this action.
11. Click **Finish**.

Configuring different alert types

For specific details about configuring each different alert type, refer to that alert action section in this chapter.

Configuring the Message Box alert action

The Message Box alert action displays a message box on the device you configure the action from. You have two options with the Message alert. You can:

- **Beep when displaying**—The message box beeps when it displays on the device.
- **Make message box system modal**—A system modal message box prevents you from working in other programs until you acknowledge the dialog by clicking on it.

Configuring the Broadcast alert action

The Broadcast alert action sends a broadcast message to everyone connected to the server generating the alert. You can configure this alert to only go to certain segments of the network by using the Advanced Discovery options. See the "Advanced Discovery" section in the online help for more information.

The Broadcast alert action will only succeed if:

1. The device receiving message has some connection to the core server, like a mapped drive.
2. The device is in the same domain and network subnet as the core server.
3. The device is set up to receive a broadcast message (on Windows 2000/2003/XP, the Messenger service must be running).

Configuring the Send Internet Mail alert action

The Send Internet Mail alert action sends an Internet mail message to the user you specify. When using the Send Internet Mail alert action, you also need to specify the SMTP Internet mail server that the alert action will send the message through.

If you specify the mail server by name, you need to have a domain name server (DNS) configured on your network so that the Send Internet Mail alert action can resolve the server's IP address. If you don't have a DNS server, enter the mail server's IP address directly.

This alert action works only if you have access to an SMTP Internet mail server at your site.

Configuring the Run Program alert action

The Run Program alert action runs a program on the device you select. If you're running a Windows program, you can select from these window states:

- Normal
- Minimized
- Maximized

The windows state option has no effect on DOS programs. Enter a full path and command line to the program you want to run. You can enter any command line options you want the program to use in the Command Line field.

Configuring the Write to Event Log alert action

The Write to Event Log alert action creates an entry in the Windows NT Event Log's Application Log. This entry is logged on the device where the alert came from. This alert action is available only on Windows NT devices.

Configuring the Load an NLM alert action

The Load an NLM alert action loads an NLM on a selected NetWare server when the AMS alert occurs. You must configure this alert to determine which NLM is loaded, and the server where it loads. This alert action is similar to the Run Program alert action for a Windows NT device.

The first time you configure this action, AMS searches the network for NetWare devices that can perform this action.

Enter the NLM to load in the NLM field. NetWare servers usually store NLMs in the SYS:SYSTEM directory. Be sure to enter the NLM path as used on the NetWare server. For example, use the system path such as SYS:SYSTEM\TEST.NLM. Don't use drive letter mappings from your device such as T:\SYSTEM\TEST.NLM because the NetWare server doesn't use these drive letters on its own hard disk.

Enter any command line options you want the NLM to use in the Command Line Options field.

Configuring the Send Page alert action

The Send Page alert action sends a pager message to the number you specify. Any device you configure a pager action on needs to have a modem. Test Send Page alert actions to make sure they work as expected. See "Testing configured alert actions" later in this chapter for more information.

Pager alert action configuration is divided into these parts:

- Configure a modem for AMS
- Configure for a paging service
- Enter a pager message

The three sections following the next procedure describe each part of the configuration process in more detail.

To configure the Send Page alert action

1. In the Configure AMS Alerts dialog, select the **parameter** you want to configure alert actions for.
2. Click **Configure**.
3. Click the **Send Page** alert action, then click **Next**.
4. Select a **client** to run the action, then click **Next**.
5. Select an **alert action severity**, or use the default setting, then click **Next**.
6. Enter the **access telephone number** you're calling. Be sure to include any numbers you need to dial to access an outside line at your site.
7. Enter the **pager ID** number.
8. Enter the **password** you use to access the paging service network in the Password field. If your paging service doesn't use a password, leave this field blank.
9. In the Service drop-down list, select your **service type**. If your paging service isn't listed, try one of the generic types. See "Configuring for a paging service" for more information.
10. Click **Next**.
11. If you're creating a message for an alphanumeric pager, type the **message text** you want to display in the Message box and move the **parameters** you want to use from the Alert Parameters list to the Message box. If you're creating a message for a numeric pager, you can only enter numbers in the Message box.
12. Enter a **configuration name**. The configuration name appears in the Configure AMS Alerts dialog beside this action.
13. Click **Finish**.

Configuring a modem for AMS

You must configure a modem for AMS to contact your paging service. You need to run the modem configuration utility and select the correct COM port and modem type settings for the Send Page alert action to function correctly.

To configure a modem for AMS

1. In Windows Explorer, double-click the **MODEMCFG.EXE** modem configuration utility. This utility is located in the WINNT\SYSTEM32\AMS_ii folder on Windows NT devices. Windows 98SE devices keep this utility in the WINDOWS\SYSTEM\AMS_ii folder.

2. From the Com Port drop-down list, select the **COM port** the modem uses.
3. From the Modem Type drop-down list, select the correct **modem** type.
4. Click **OK** to save these settings. Your modem is configured to work with the AMS alerting system.

Configuring for a paging service

You can access a paging service either directly or indirectly, though AMS Send Page alerts only work with direct paging services.

Paging method	Description
Direct paging	Refers to dialing the paging service provider's network access phone number. You access their device network to enter the pager identification number, and the paging service network then sends the message to the pager.
Indirect paging	Requires calling a paging service, speaking with an operator, and giving the operator the pager's identification number. AMS Send Page alerts don't work with indirect paging. Because the paging service operator enters the information into the paging network that sends the message to the pager, the AMS message can't get through to the paging service network. The indirect paging method, sometimes used when contacting the network directly, is a toll call, and the pager service offers toll-free service through the operator.

You need to configure the Send Page alert action for your paging service. At a minimum, this information includes the paging service phone number and the name of the paging service you're using.

Always put the paging service's phone number in the Send Page dialog's Service Provider field. If your paging service isn't in the Send Page dialog's Service drop-down list, try using the Generic Beeper or the Generic Alphanumeric service (pick the one that matches the type of pager you're using). Put the password you use to access the paging service network in the Password field.

If the generic service doesn't work with your pager

You must configure the communication parameters for the Send Page alert action. This information includes the baud rate, data and stop bits, parity, and paging protocol your paging service uses. This information is available from your paging service. If your paging service is in the Service drop-down list, these parameters are configured automatically when you select the service.

To configure your paging service manually, see the following procedure.

To configure the Pager alert action for an unlisted paging service

1. In the Pager dialog's Service field, click **New**.
2. Click **Properties**.
3. Enter the **maximum message length, baud, data bits, stop bits, parity, and protocol** that your paging service requires. You can get this information from your paging service.
4. Click **OK**.
5. Click **Next**.
6. If you're creating a message for an alphanumeric pager, type the **message text** you want to display in the Message box and move the **parameters** you want to use from the Alert Parameters list to the Message box. If you're creating a message for a numeric pager, you can only enter numbers in the Message box.

7. Enter a **configuration name**. The configuration name appears in the Configure AMS Alerts dialog beside this action.
8. Click **Finish**.

Entering a pager message

The Pager alert action supports both alphanumeric and numeric-only pagers (often called beepers).

If you're paging an alphanumeric pager, the message can include any text you type in and information from the alert that generated the message. This message shouldn't exceed the maximum number of characters your paging service supports; otherwise, you could get a truncated message.

Paging with a numeric-only pager

If you're paging with a numeric-only pager, you can only send numbers. Create a system of server numbers and numeric error codes that corresponds to alerts you configure. For example, create a system where **1** refers to your production server and number **101** means the disk is almost full. When you receive message **1 101**, you'd know that your production server's disk is almost full.

Configuring the Send SNMP Trap alert action

Simple Network Management Protocol (SNMP) is a message-based protocol based on a manager/agent model consisting of Get, GetNext, and Set messages and responses. SNMP uses traps to report exception conditions such as component failures and threshold violations.

AMS can generate an SNMP trap when an alert happens. You can configure systems generating alerts to send these traps to an SNMP management console if you have one.

SNMP event console not included

Management Suite does not include an SNMP event console for viewing SNMP traps and events.

To configure the Send SNMP Trap alert action

1. In the Alert Settings dialog, select the **parameter** you want to configure alert actions for.
2. Click **Configure**.
3. Select the **SNMP Trap** alert action, then click **Next**.
4. Select a **client** to run the action, then click **Next**.
5. Select an **alert action severity**, or use default, then click **Next**.
6. Type any message text you want to display in the SNMP trap and move available parameters you want from the Alert Parameters list to the Message box.
7. Enter a **configuration name**. This name appears in the Alert Settings dialog beside this action.
8. Click **Finish**.

You must specify the trap destination address (either IP or IPX) of the devices that you want SNMP traps sent to.

To install SNMP on Windows 2000

1. From the Windows 2000 Control Panel, double-click **Add/Remove Programs**.
2. On the left of the window, click **Add/Remove Windows Components**.
3. Select **Management and Monitoring Tools** and click **Details**.

4. Select **Simple Network Management Protocol** and click **OK**.
5. Click **Next**.
6. Windows 2000 will install the SNMP component. Complete the SNMP installation.

To configure trap destinations for Windows 2000

1. In Control Panel's Computer Management applet, click **Services and Applications** and **Services**.
2. Double-click the **SNMP Service**.
3. Click the **Traps** tab.
4. In the **Community Name** list, enter **Public** and click **Add to list**.
5. Enter the **Trap Destinations** for the devices you want traps sent to, then click **Add**.
6. Click **OK**.

To configure trap destinations for Windows NT 4

1. From the Windows NT Control Panel, double-click the **Network icon**.
2. Click the **Services** tab.
3. Click the **SNMP Service item**, then click **Properties**.
4. Click the **Traps** tab.
5. In the Community Name drop-down list, select **public**. If there's no public entry in the list, type it in, then click **Add**.
6. After you've selected or entered the "public" community name, click **Add** below the Trap Destinations list.
7. Enter the **addresses** of the devices you want traps sent to, then click **Add**.
8. Click **OK** | **Close**.

To configure trap destinations for NetWare 5.1 servers

1. From the NetWare server console, type:
load install
2. Click **Product Options**.
3. Click **Configure Network Protocols**.
4. Click **Protocols**.
5. Click **TCP/IP**.
6. Click **SNMP Manager Table**.
7. Enter the **addresses** of the devices you want traps sent to, then click **Add**.

Working with configured alert actions

After you configure alert actions, you can test them to make sure they work as expected, you can delete them, or you can export them to other devices.

Testing configured alert actions

After you configure alert actions, test them in the Alert Settings dialog.

To test configured alert actions

- Right-click an **alert**, then click **Test action** to test all alert actions configured for that alert. Right-click a specific **alert action**, then click **Test action** to run only that alert action.

Deleting alert actions from a parameter

You can delete an alert action from a parameter.

To delete an alert action from a parameter

1. In the Alert Settings dialog, right-click the **alert action** you want to delete.
2. Click **Delete**.

Exporting alert actions to other devices

Each device that generates AMS alerts stores its alert information in a local AMS database. Normally, the alerts and actions stored in one database aren't visible to AMS databases on other devices. There may be times when you want to duplicate configurations of AMS alert actions across multiple devices so you don't have to repeat your work. The AMS export option lets you export alert actions to other devices that generate AMS alerts.

Some alert actions may not work on other devices. For example, if you export a Send Page alert action to a device that doesn't have a modem, the alert can't work.

When you export alert actions from one device to another, you can export a single alert action or all alert actions.

To export alert actions to other devices

1. From the **Alert settings** dialog, right-click on an **alert category** and click **Export**.
2. Check the alert categories or alert actions you want to export. Click **Next**.
3. In the **Select computers** dialog, select the computers you want to receive the alert actions you selected. If the device you want has AMS active on it and it isn't in the **Available computers** list, click **Refresh** to rediscover devices with AMS.
4. Click **Finish**.
5. In the **Export status** dialog, verify that the alert actions exported successfully.

Viewing export status

After AMS exports alert actions to the devices you selected in the Select Computers dialog, AMS displays the export results in the Export Status dialog. This dialog displays alert actions that don't export successfully. If alerts don't export successfully, it can be for these reasons:

- AMS isn't installed or working correctly on the target device. Verify AMS by testing a configured alert action on that device from the Alert Settings dialog.
- The alert that the action was configured for doesn't exist on the target device. Make sure that the application that registered the alert with AMS on the source device is installed on the target device.

Viewing the AMS Alert History

You can use the console Alert History to view a list of all AMS alerts generated by devices on the network. You can configure the Alert History to display:

- Only those alerts that match conditions you specify
- A specified number of entries

The list of alerts is displayed in the Alert History dialog with this information about each alert:

- Alert Name
- Source
- Computer
- Date
- Time
- Severity

In addition to the basic information the Alert History dialog displays, you can access more detailed information about each alert in the Alert Information dialog. The core server stores the AMS Alert History information for all device workstations and consoles.

To view the Alert History

- In the console, click **View | Alert History** to see the Alert History.

Filtering the Alert History display list

You can configure the Alert History to display only those alerts that match criteria you specify. You can filter which alerts display according to these parameters:

Filter	Description
View From/View To	Sets the date and time range of alerts.
Computer	Displays alerts from a specific device.
Source	Displays alerts from the same type of alert source (such as Remote Control Agent) on one or more devices.
Alert	Displays all alerts with a specific alert name.
Severity	Displays only alerts matching the severity levels you select. You can specify these severity levels: Monitor, Information, OK, Non-Critical, Critical, and Non-Recover.

To specify which alerts display in the Alert History

1. Right-click in the **Alert History** window, then click Options.
2. On the Filters tab, select the filters you want to apply to the Alert History list.
3. Click **OK**.

To change the number of entries displayed in the Alert History

1. Right-click in the **Alert History** window, then click Options.
2. On the **Settings** tab, specify the number of log entries you want the log to hold.
3. Click **OK**.

Viewing detailed alert information

You can view detailed information about each alert the Alert History window displays. The detailed information appears in the Alert Information dialog and includes alert parameters, their values, and the action status of each alert.

The Alert Information dialog also displays this information:

Action Status Description

Action Type	Type of action generated by the alert, such as Message Box, Pager, Internet Mail, Execute Program, or Broadcast.
Action Name	Name given to the specific action.
Computer	Name of the device where alert was configured to occur.
Status	Alert status, such as pending, processing action, error, completed successfully, or failed to complete.

To view alert information

1. From the Alert History window, double-click the **alert** that you want to display detailed information for.
2. When you finish viewing the alert information, click **Close**.

The device listed in the Alert History is the core server that recorded the action; it records all events.

To see which device generated an alert

- Double-click the **Alert History entry** you want more information about. The Alert Information window displays additional alert details including the name of the device that generated the alert.

Deleting Alert History entries

You can delete entries in the Alert History either individually or as a group.

To delete a single log entry

- Select the log entry you want to delete, right-click in the **Alert History window**, then click **Delete | Selected Entries**.

To delete multiple log entries

1. While pressing the **Ctrl key**, select the log entries you want to delete.

-
2. Right-click in the **Alert History window**, then click **Delete | Selected Entries**.

To delete all visible log entries

1. Filter the Alert History so that only the entries you want to delete are visible.
2. Right-click in the **Alert History window**, then click **Delete | Filtered Entries**.

Copying Alert History contents to the clipboard

You can copy Alert History entries and their parameters to the clipboard so you can then paste them to another application for printing or data analysis.

Only parameters visible in the log are copied. To limit the number of entries the Alert History copies to the clipboard, apply filters to limit the number of visible log entries.

To copy Alert History contents to the clipboard

1. Adjust the **log filters** so that only the entries you want to copy are visible.
2. Right-click in the **Alert History window**, then click **Copy**.

Using the Asset Manager add-on

LANDesk Asset Manager is a complete asset management solution that lets you record, track, and analyze any type of fixed asset within your organization—including IT assets like computers and monitors, office equipment, furniture, and any other valuable item you want to manage—in addition to critical business information such as contracts, invoices, and projects.

Asset Manager includes all the tools you need to configure data entry forms, enter items into the database with those forms, as well as collect and analyze that data with customizable reports.

For two of the predefined asset types, computers and software, Asset Manager also provides the capability to link and update asset data from the scanned inventory and SLM records.

Asset Manager is a Web-based application that runs in the LANDesk Web console. Note that Asset Manager is supported only in the Internet Explorer browser, and that Asset Manager is not accessible in the main Windows console.

Asset Manager 8 Add-On

Asset Manager is a separately purchased add-on product that integrates seamlessly with your current LANDesk network. If you haven't purchased or installed a LANDesk Asset Manager license, the user interface and the capabilities described here are not on your core server and will not be available from the Web console.

For information about purchasing an Asset Manager license, visit the LANDesk Web site.

For information about installing and activating the Asset Manager add-on product, refer to "Installing add-ons" in the *Installation and Deployment Guide*.

Read this chapter to learn about:

- Asset Manager overview
- Using role-based administration with Asset Manager
- Accessing Asset Manager in the Web console
- Managing assets
 - Working with computer assets
 - Working with software assets
- Managing contracts
- Managing invoices
- Managing projects
- Managing global lists
- Using subgroups to organize types
- Creating new types
 - Using a details summary
 - Adding details
 - Adding detail tables
 - Managing detail templates
 - Adding detail templates
 - Organizing details in sections
- Using an item list
- Adding items to the database
- Using asset alert dates
- Associating items
- Importing items
- Exporting items

USER'S GUIDE

- Searching for items
- Using Asset Manager reports

Asset Manager overview

Asset Manager adds easy-to-use features to the Web console that let you proactively manage all types of fixed (non-scannable) assets across your enterprise throughout the entire asset life cycle. In addition to physical assets, you can manage other relevant information such as contracts, invoices, and projects. If implemented and maintained properly, this type of information management can provide the security, access, and control of important data necessary to not only make informed business decisions and planning, but improve the productivity and efficiency of your organization's everyday business operations.

In short, Asset Manager helps you get the most out of your IT investments.

Linked data from the core database (for computers and software)

With Asset Manager, you can leverage existing data for computers and licensed software products that has already been scanned (via the inventory scanner) or entered manually into your core database.

Import and export capabilities

You can also use Asset Manager to import and export asset data to use with other data tracking and management applications and databases. The import and export features support both CSV (comma-separated value) and XML formatted files.

Other features and benefits

In addition to the features mentioned above, with Asset Manager you can:

- Use predefined types (i.e., data entry forms) or create your own custom types that are used to add items to the database.
- Store asset management data in a single repository—the core database. A single database simplifies data management, ensures data accuracy and integrity, and allows multiple users to enter asset data and generate reports at the same time.
- Associate assets with each other and with other related information, such as invoices, users, service histories, etc.
- Set up alert dates to automatically notify you when an asset's pre-established deadline expires.
- Use predefined asset management reports or create your own custom reports.
- Reconcile recorded asset data with actual physical inventories.
- Track asset data history.

Understanding Asset Manager types and details

Asset Manager uses types and details to describe the kinds of items (and their inherent properties) that can be added into the database. A *type* simply represents a specific kind of asset, contract, invoice, project; and so on. And a *detail* represents specific information about that type. To understand this concept in practical terms, it's probably helpful to think of a type as essentially a data entry form (made up of details) for a particular kind of item, and each detail as an individual data field on the form.

Asset Manager has several predefined asset types, contract types, invoice types, project types, and global list (or universally applicable) types, each defined by its own unique combination and arrangement of details. However, you're not limited to these types or details. With Asset Manager, you can also create and modify your own custom types, details, detail tables, and detail templates in order to meet your asset management requirements and goals. You're able to determine the content and layout of a data entry form, what type of information is being asked for, whether a data field is required, and more.

Ultimately, the purpose of asset types and details is to give you a way to configure data entry forms that you then fill out in order to add items to the database.

Asset management workflow

The following steps provide a quick summary outline of the typical processes involved in implementing an asset management strategy on your LANDesk network. Each of these tasks is described in detail in the appropriate sections of this chapter.

1. Managing types (viewing, organizing, editing, and deleting) with the Assets, Contracts, Invoices, Projects, and Global Lists pages.
2. Creating types (i.e., data entry forms) with the Add new type page.
3. Creating details (i.e., data fields) for types with the Add details page. Also, adding detail tables and detail templates to types.
4. Adding items to the database by filling out data entry forms.
5. Importing and exporting asset items.
6. Using predefined and custom reports to collect and analyze asset data.

Using role-based administration with Asset Manager

Role-based administration is LANDesk's access and security model that lets LANDesk Administrators restrict access to tools and devices. Each user is assigned specific rights and scope that determine which features they can use and which devices they can manage. For more information about role-based administration, see *Using role-based administration in the Users Guide*.

Role-based administration can also be implemented to control access to features in the Web console, including the Asset Manager tool. To learn more about how role-based administration works for the basic Web console interface and tools, see *Using the Web console in the Users Guide*.

Asset Manager introduces three new roles and corresponding rights to role-based administration. An administrator assigns these rights to other users with the Users tool in the main console (see the *Users Guide* for details). In order to see and use the various Asset Manager features in the Web console, a user must be assigned the necessary Asset Manager right, as described below.

Note: In addition to users that have only one of the rights below, a user could have both the Asset Data Entry and Reports rights. Since Asset Configuration gives full access to Asset Management, any combination with it would be redundant.

Asset Configuration

The Asset Configuration is an administration-level right that provides users the ability to:

- See and access all the Asset Management links in the Web console: Assets, Contracts, Invoices, Projects, Global Lists, Detail Templates, and Reports.

- Create new types
- Edit types (both predefined and custom)
- Delete types
- Create, edit, and delete subgroups used to organize types
- Create new details for types
- Edit details (both predefined and custom)
- Create and modify detail templates
- Create and modify detail tables
- Create, edit, and delete sections used to organize details
- Perform all of the Asset Manager tasks allowed by the other rights listed below

Asset Data Entry

The Asset Data Entry right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, and Global Lists links in the Web console.
- Browse types and details (can't add, edit or delete them)
- Add items to the database by filling in data entry forms
- Edit items that have been added to the database

Reports

The Reports right for asset management-specific reports is the same Reports right that allows users to generate and view all other reports in the main console. This right provides users the ability to:

- See and access the Assets, Contracts, Invoices, Projects, Global Lists, and Reports links in the Web console.
- Browse types, details, and items (can't add, edit or delete them)
- Run predefined Asset Manager reports
- Create and run custom asset reports
- Edit all report configurations
- Print all reports

Accessing Asset Manager in the Web console

Asset Manager is a browser-based application that is accessed through the Web console (note that Asset Manager is supported only in the Internet Explorer browser). Asset Manager features and interface do not appear at all in the main Windows-based console. In order to use Asset Manager, you must already have the Web console software installed on either your core server or on another Web server on your network.

For more information about the Web console

For information on installation prerequisites and procedures for the Web console, see Installing the Web console in the *Installation and Deployment Guide*.

For more information on logging in to the Web console and using the default Web console features, see Using the Web console in the *Users Guide*.

Users with a valid Web console account can access Asset Manager in the Web console from any Windows-based computer running Internet Explorer 5.5 or later.

To access Asset Manager in the Web console

1. From a networked computer, open Internet Explorer.
2. In the Address field, enter the URL to the site hosting the Web console pages. Normally the URL is: `http://webservername/remote`.
3. Once you authenticate, an Asset Manager link appears in the left navigation pane. Clicking on this link will open Asset Manager in its own browser window, with features displayed based on the user's role based administration rights.

What's next?

Now that you have a basic understanding of what you can do with Asset Manager and have logged into the Web console, you can click any of the Asset Management links and start using the features introduced in this overview section.

Online help

From any page in the Web console, including Asset Manager pages, click the Online Guide link in the upper right corner to access online context-sensitive help for that page.

Managing assets

The Assets page shows all the asset groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Assets are defined as IT items or property that can't be scanned by the inventory scanner into the core database but that you want to track and manage, such as printers, monitors, phones, desks, supplies, etc. The exception to this definition are the computer and software types (see below for an explanation about these two special asset types). There's no limit to the number or variety of IT assets you can record with Asset Manager.

Asset *types* represent the data entry forms used to enter asset items into the database. You can use the predefined asset types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the **Add Type** link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) **Add** link and filling out the data entry form.

The predefined asset groups and types include:

Miscellaneous

- Chair
- User

Office Equipment

- Copier
- Digital Camera
- Fax
- Mobile Phone
- Phone
- Projector
- Television

Technology

- Computer
Important: Computer is a special asset type because it contains linked data that can be updated and synchronized with inventory data in the core database. The computer asset type can't be deleted or renamed. For more information, see [Working with computer assets](#).
- Monitor
- PDA
- Printer
- Router
- Scanner
- Software
Important: Software is a special asset type because it contains linked data that can be updated and synchronized with inventory data. The software asset type can't be deleted or renamed. For more information, see [Working with software assets](#).
- Switch

Working with computer assets

The computer type is one of two asset types with linked details (data fields) that can be updated and synchronized with information from the core database. Designated computer type details are linked to a scanned device's hardware inventory (a scanned or managed device is one on which the Management Suite inventory scanner has been run). The other asset type with linked details that can be updated with information from the core database is the software type.

You can use linked details to populate linked data fields for computers that have already been scanned and have an inventory record. For computers that aren't yet connected to your network or haven't yet been scanned by the inventory scanner, you can manually add computer items in Asset Manager (using a valid MAC addresses or serial number provided by the manufacturer), and populate the other linked data fields after the machines have been scanned.

The computer asset type can't be deleted or renamed.

Linked details for computers

Only designated computer details are linked and can be updated from a scanned computer's hardware inventory. These details are identified by the linked-chain icon. Linked details can't be deleted, and you can't create your own linked details.

The following computer details are linked:

- Device ID

Important: The Device ID linked detail can be thought of as the master link because it is used to definitively identify each specific computer asset in the hardware inventory, ensure there are no duplicate records, and synchronize the appropriate linked data for each computer asset. Device ID is listed as a Hidden information type in the computer details summary page, and only its Default value and Summary fields can be edited manually.

- Machine name
- Manufacturer
- MAC address
- Serial number
- Model
- Asset tag
- Domain name
- Description
- Notes
- Last hardware scan date
- Primary owner (the user who has logged in to a device the most times within a specified number of logins. The default number of logins is 5.)

All other details for the computer type are not linked and must be entered and updated manually.

You can manually enter information in linked data fields only BEFORE updating those details with inventory information. Once a computer's linked data has been updated, the linked data fields can no longer be edited manually. However, you can refresh/update linked data from the inventory as many times as you like.

Non-linked data fields can always be edited in Asset Manager. Non-linked data does not appear in a scanned device's inventory tree.

Updating linked data for computers

You can update all of your scanned computers at once from the computer item list page (this may take a long time depending on how many managed devices you have in the core database). Or, you can update linked data for an individual computer from its own page.

Asset inventory update utility

You can also update both computer and software asset data at the same time with a utility executable installed on the core server by the Asset Manager setup program. You can use this utility to update asset data manually or as a scheduled task with Windows Task Scheduler. For more information, see [Using the asset inventory update utility](#).

To update the computer item list

1. From the Assets page, open the **Technology** subgroup, and then click **Computer** to view all the computer assets currently recorded in the database.
2. Click the **Refresh asset data** link located above the computers list.

Scanned devices that do not have a corresponding computer item on this page are added to the list, with their linked data fields filled in. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

If a corresponding computer item already exists on this page, its linked data is refreshed/updated from the scanned device's inventory. If the information has changed in the inventory, the new information replaces the value in the linked data field. Only linked data fields are updated.

To update linked data for one computer item

1. From the computer item list page, edit the computer by clicking its pencil icon.
2. Click the **Refresh asset data** link located above the details list.

The computer's linked data is updated with information from the corresponding scanned device's inventory. This process rewrites any manually entered or changed value in a linked data field with the current value in the inventory. Empty linked data fields are filled in, if that data exists. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

From a specific computer's page, you can also click the **Open inventory data** link located above the details list to view the scanned device's entire inventory tree.

Note: If the Open inventory data option is not available on a computer's page, it indicates the corresponding device has been deleted from the hardware inventory. When a device is deleted from the inventory, its asset record is not removed from Asset Manager.

Using the asset inventory update utility

When you install the Asset Manager add-on, an utility executable is copied to the LDMain folder on the core server (the LANDesk\ManagementSuite folder). This utility provides the convenience of being able to refresh all of the computer and software license asset data that currently resides in the core database at once, either manually or as a scheduled task at a specific time. In other words, you don't have to perform this task via the computer or software item list pages in the Web console's Asset Manager pages.

The name of the executable file is:

LANDesk.ManagementSuite.AssetManagement.InventoryUpdate.exe

You can run this utility by any of the following methods:

- Double-click the executable file
- Run the executable from a command line interface
- Create a Windows Scheduled Task that runs this executable. Note this is NOT a LANDesk Scheduled Task.

To create a Windows Scheduled Task to update (refresh) computer and software asset data

1. At the core server, click **Start | Programs | Accessories | System Tools | Scheduled Tasks**.
2. Click **Add Scheduled Task** to open the Scheduled Task wizard, and then click **Next**.
3. Use the **Browse** button to locate and select the utility executable (named above) in the ManagementSuite folder, and then click **Next**.
4. Enter a name for the task, select the frequency when the task should be performed, and then click **Next**.
5. If necessary, select the time and day when the task should be performed, and then click **Next**.
6. Enter the user name and password for a valid LANDesk Administrator user, and then click **Next**.
7. Click **Finish**. The task should appear in the Scheduled Tasks window. (You can right-click a task to run it, delete or rename it, or to modify any of the task's basic or advanced settings.)

Working with software assets

The software type is one of two asset types with linked details (data fields) that can be updated and synchronized with information from the core database. Designated software type details are linked to license file information for your licensed software products. The other asset type with linked details that can be updated with data from the core database is the computer type.

You can use linked details to populate linked data fields for software that has a license file recorded in Software License Monitoring (SLM) in the main console or in the Compliance section in the Web console. For more information about the SLM tool, refer to the *Users Guide*.

The software asset type can't be deleted or renamed.

Linked details for software

Only designated software details are linked and can be updated from SLM. These details are identified by the linked detail icon. Linked details can't be deleted, and you can't create your own linked details.

The following software details are linked:

- Product name
- Version
- Publisher
- Product Link ID

Important: The Product Link ID linked detail can be thought of as the master link because it is used to definitively identify each specific software asset in SLM, ensure there are no duplicate records, and synchronize the appropriate linked data for each software asset. Product Link ID is listed as a Hidden information type in the software details summary page, and only its Default value and Summary fields can be edited manually.

- License number
- License type
- Quantity
- Serial number
- Purchase date
- Unit price
- Order number
- Reseller
- Owner
- Location
- Note

All other details for the software type are not linked and must be entered and updated manually.

You can manually enter information in linked data fields only BEFORE updating those details with SLM information. Once a software product's linked data has been updated, the linked data fields can no longer be edited manually. However, you can refresh/update linked data from the product information in SLM as many times as you like.

Non-linked data fields can always be edited in Asset Manager.

Updating linked data for software

You can update all of your software products that have a valid license file at once from the software item list page. Note that not all of your licensed software products in SLM necessarily have a license file. Only those licensed products with an actual license file will be updated. Or, you can update linked data for an individual software product (that has a license file) from its own page.

Asset inventory update utility

You can also update both computer and software asset data at the same time with a utility executable installed on the core server by the Asset Manager setup program. You can use this utility to update asset data manually or as a scheduled task with Windows Task Scheduler. For more information, see *Using the asset inventory update utility*.

To update the software item list

1. From the Assets page, open the Technology subgroup, and then click **Software** to view all the software assets currently recorded in the database.
2. Click **Refresh asset data** link located above the

Software products (with a license file) that do not already have a corresponding software item on this page are added to the list, with their linked data fields filled in. If there is no data the field is left blank, and can't be edited.

If a corresponding software item already exists on this page, its linked data is refreshed/updated from the license file information in SLM. If the information has changed in SLM, the new information replaces the value in the linked data field. Only linked data fields are updated. If there is no data the field is left blank, and can't be edited.

To update linked data for one software item

1. From the software item list page, edit the software product by clicking its pencil icon.
2. Click **Refresh asset data** link located above the details list.

The software product's linked data is updated with information from the corresponding product's license file information in SLM. This process rewrites any manually entered or changed value in a linked data field with the current value in SLM. Empty linked data fields are filled in, if that data exists. If there is no data, the field is left blank and can no longer be edited manually, although it can be filled in by a later update.

Managing contracts

The Contracts page shows all the contract groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Contracts can be any sort of document pertaining to the formal business relationships you have with service providers, partners, and vendors that you want to record and manage. Record critical information about the contract such as names, effective dates, status, contract numbers, terms and conditions, relationships, etc., and then associate the contract with the assets it covers. For example, you could enter data about a lease agreement for a group of printers, and then associate the lease with the printers.

Adding contract information to the database not only helps you keep track of valuable assets but also the important information you need for negotiating terms and conditions for future contracts.

Contract *types* represent the data entry forms used to enter contract items into the database. You can use the predefined contract types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined contract groups and types include:

Standard

- Consulting Agreement
- Escrow
- Lease

Managing invoices

The Invoices page shows all the invoice groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Invoices are documents pertaining to the purchase, acquisition, or payment of products and services. With Asset Manager, you can enter and store relevant information about an invoice and associate it to the corresponding asset.

Invoice *types* represent the data entry forms used to enter invoice items into the database. You can use the predefined invoice types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined invoice groups and types include:

Standard

- Invoice
- Purchase Order

Managing projects

The Projects page shows all the project groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Large, complex projects typically involve the purchase and use of a variety assets and related materials. With Asset Manager, you can enter specific project information into the database, associate the project with any other recorded item, and then generate custom reports to help you track and manage the project.

Project *types* represent the data entry forms used to enter project items into the database. You can use the predefined project types or create your own.

From any of the type pages, you can:

- View types in subgroups, as well as by global lists.
- Create, edit, and delete subgroups by clicking the Manage subgroups link.
- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined project groups and types include:

Miscellaneous

- Ad hoc

Standard

- Capital Expenditure
- Sustaining

Managing global lists

The Global Lists page shows all the global list groups and types. You can expand and collapse groups by clicking the group name, or by clicking the Expand All and Collapse All links.

Global lists refer to lists of standard information, such as locations, companies, and users, that can be applied globally to describe assets throughout your organization. By defining these global lists in one place, and using them to add standard data to other types, you can ensure consistent usage in all your asset management records. For example, if you need to update data in a global list, such as a department's name or company's address, the new information propagates automatically to all other items that include that standard global list data.

Global List *types* represent the data entry forms used to enter global list information into the database. You can use the predefined global list types and create your own custom global list types.

On a data entry form, an Expand/Collapse icon next to a data field's text box identifies it as a global list type that can be used to select a detail from a list of that global list type's available details. Whereas, an Expand/Collapse icon next to a data field name, where there is no text box, identifies a table detail.

Using global lists to add a detail to a type

Global lists are different from the asset, contract, invoice, and project types because you can use a global list type to add a standard detail (or data field) to any of the other types. For example, let's say you're adding a detail to a new asset type; choosing "Global List" opens a new dialog where you can select the global list type called "locations" (and, if you want to specify a default value, you can also select a specific location from the drop-down list of available locations). In this way, global list types are truly global, meaning they're available for all other types, and provide standard, consistent information across the database's asset records.

As previously mentioned, if a detail in a global list type is changed, the change is reflected in any recorded item that uses that detail.

Using global lists to organize and view types

Global lists serve another unique purpose in Asset Manager. They can be used as parent groups to view lists of asset, contract, invoice, and project types. From any of the type pages, you can click the **Group by** drop-down list and select a global list (predefined and custom) by which to arrange the types on that page.

For example, if you want to view computer asset types by location, select the "location" global list. Each current location appears as a parent group that can be expanded to show the types (in their subgroups) with matching location data. Types that do not contain location data are listed under the "No Information" parent group. If there aren't any types in the "location" global list type, the "No Information" parent group displays, containing all the page's subgroups and types.

If you select **None** from the Group by menu, subgroups and types are listed without a parent global list group. None is the default setting.

As with other type pages, from the Global Lists page you can:

- View types in subgroups. (Grouping by global list types is not supported on the global lists page.)
- Create, edit, and delete subgroups by clicking the Manage subgroups link.

- Check the count of items currently recorded in the database for each type.
- Print the selected view of groups and types.
- Search for types in the list.
- Edit a type's details, or add new details, by clicking the pencil icon next to the type to access its details summary page.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Create new types in a subgroup by clicking the Add Type link.
- Rename types by clicking the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)
- View a list of all the items that have been added to the database for a particular type by clicking the type name.
- Add items to the database by clicking the plus sign (+) Add... link and filling out its data entry form.

The predefined global list groups and types include:

Default

- Company
- Cost Center
- Department
- Location
- Vendor

Displaying large global lists

The more items you place in a global list, the longer it takes for a page containing that global list to display. For example, when a global list is included in a specific type's definition, that type's Add Items and Edit Items data entry pages take longer to display. Also, selecting a global list that contains a large number of items in the Group By drop-down list may take longer to display.

Creating new types

Use the Add new type page to create your own custom types for assets, contracts, invoices, projects, and global lists.

As a reminder, it might be helpful to consider types as data entry forms comprised of specific details that define an item. Types are divided into the following five major categories in order to facilitate tracking and reporting: Assets, Contracts, Invoices, Projects, and Global Lists. For example, a printer is an asset type, a lease is a contract type, and a location is a global (i.e., generally applicable) type. To continue the example, a printer asset type could be comprised of details (data fields) specifying the printer's manufacturer, model, description, service history, warranty type, cost, and so on. A type is used to add items to the database.

Asset Manager comes with several predefined types that can be used to add common items to the database. You also have the flexibility to create as many additional custom types as you like to accommodate all of the IT assets and critical information you want to manage.

The first step in creating a new type is to define the type's key detail. After the key detail is defined you can add as many other details as you like. All types are created by the same procedure, described below.

To create a new type

1. From any Asset Manager type page (Assets, Contracts, Invoices, Projects, Global Lists), click the **Add type** link next to the group where you want to add the type.
2. In the **Type name** field, enter a unique name for the type.
3. In the **Key name** field, enter a name for the key detail. Every type must have one (and only one) detail designated as the "key" so that it can be tracked in the database. When you initially create a new type, you're required to specify the name of its key detail. If the key detail is the only detail for a type, it must also be a unique and required value.

Once a type is created you can't delete its key detail. Additionally, once designated you can't change a type's key detail to be another detail.

4. From the **Type** drop-down list, select the type of information you want this type's key detail to represent. Available kinds of information include: String (alphanumeric characters or symbols), Integer (whole number), Date (calendar date), Decimal (real number that allows two decimal places; the decimal point separator can be either a period or a comma), and Alert Date (calendar date; for more information, see Using asset alert dates).

Note: Static List and Global List are not valid information types for the key detail. However, they can be used when creating additional details. For more information, see Adding details.

5. If you selected the String type, you must specify the maximum number of characters allowed in the string by entering a numerical value in the **Length** field. The valid range is from 1 to 4,000 characters for English and other European languages (the range is from 1 to 2,000 characters for supported double-byte Asian languages). This field is required for a string and is not available for any other information type.
6. Again, if you selected the String type, you can enter a required format or syntax in the **Input Mask** field. This field only applies to strings and is optional.

The input mask indicates a required format when entering data for this detail on a data entry form. For example, if the detail is a serial number that must conform to a certain format such as "abc-123456" you would enter an input mask like this: aaa-#####, where lower-case "a" represents any letter, the hyphen is a literal character, and the pound character (#) represents a number. For the actual character a, use the /a exception. For the actual pound character (#), use the /# exception. This mask appears on the data entry form so the user knows how to enter data for the field.

Note: Only the alphanumeric characters a-z, A-Z, and 0-9 are supported when filling in a string detail on a data entry form whose required syntax is specified by an input mask. Extended characters and double-byte characters are NOT supported.

7. If you want to specify a value that will automatically appear in the key detail's data field on a data entry form, enter that value in the **Default Value** field. You can enter a default value for any type of information. This field is optional. (To enter a default date value, use the calendar control.)

Note: Any default value specified here can be changed when filling out the actual data entry form.

8. Click **Save** to save the type and its key detail, and to return to the Details for... page.

At this page you can continue to configure the type by adding more details, detail tables, or detail templates. You can also change the subgroup where this type resides with the **Belongs to** drop-down list.

9. **Important:** When you're done configuring the type, you must also click **Save Details** on the Details for... page in order to save all the details you've added to that type.

Once a custom type is created, you can:

- Edit a type's details by clicking the pencil icon.
- Delete types by clicking the X icon. (You can delete a type only if it doesn't have any items recorded.)
- Add items to the database by clicking the plus sign (+) **Add** link and filling out the data entry form.

Using a details summary

This page provides a summary view of all the details that make up the type named at the top of the page. A type's details are what appear on a data entry form for that type.

Each type's details summary page is unique, depending on the details that have been used to define that type. However, the tasks you can perform from any details summary page are the same.

From any details summary page, you can:

- View all the details that define the selected type.
- Edit existing details by clicking the pencil icon next to the detail name.
- Create new details for a type by clicking the Add detail link.
- Create an alert date detail for a type.
- Add a group of details to a type at once by clicking the Choose template link.
- Add a table data field to a type by clicking the Add table link.
- Delete a detail by clicking the X icon.
- Organize details in configurable sections by clicking the Manage sections link.

Important note on saving changes to details:

In order to preserve any changes you've made to details in the details summary list (including changes to detail templates and detail tables), you must always click **Save Details** on this page. If you add, modify, or delete one or more details and then click **Cancel** on this page, none of your changes will be saved.

Understanding the detail icons

The details summary page includes a legend with icons that indicate different characteristics for the detail. Detail icons appear here in a details summary list, as well as on an item page and on data entry forms next to data fields.

The legend shows the following icons:

Key: Indicates the detail is the key identifying detail for this type. Each type must have one, and only one, key detail in order to be saved. Key details are automatically unique and required. A key detail can't be deleted or changed.

Unique: Indicates the detail must have a unique value entered when filling out the data entry form. If you enter a duplicate entry (the same value already exists in that data field for another item), an error message displays. Unique details are automatically required. Types can have multiple details that ask for unique data.

Required: Indicates the detail must have valid data entered when filling out the data entry form. A required detail may or may not be unique. For example, if a detail is marked required but not unique, you can enter the same data in that field on data entry forms for different items.

Summary: Indicates the detail will appear as a column heading on an item list page.

Linked: (Applies only to the computer and software asset types) Indicates the detail is linked to corresponding scanned device data, or entered software license data, in the core database. The linked characteristic applies to only some of the details for the computer and software asset types, not all of their details. The linked characteristic does not apply to any details for any other asset type. You can't create your own linked details.

Asset Manager lets you update and synchronize linked data by using the computer or software asset's Refresh feature. Computer assets are updated with the current device inventory data that has been scanned into the core database by the inventory scanner. Software assets are updated with the licensed software products data you've entered into the core database.

Adding details

Use this page to add a new detail, or edit an existing detail, for an asset type.

Details represent the data fields on an item's data entry form. When you fill out a data entry form, that item is added to the core database and can be tracked and managed with Asset Manager.

To edit an existing detail, click the pencil icon next to the detail name. For a description of what information you can and can't edit on a saved detail, see Rules for editing details below.

To add a new detail

1. From any details summary page, click the **Add detail** link.
2. In the **Name** field, enter a unique name for the detail.
3. From the **Type** drop-down list, select the type of information you want this detail to represent. Available kinds of information include: String (alphanumeric characters or symbols), Integer (whole number), Date (calendar date), Decimal (real number that allows two decimal places; the decimal point separator can be either a period or a comma), Alert Date (calendar date; for more information, see Using asset alert dates), Static List (lets you create a predefined list of values; see the Static List step below), and Global List (lets you select any of the current global list types; see the Global List step below).
4. The **Key** option is not available because this is not the initial detail. The key detail is defined when you initially create the type, and it can't be changed or removed.
5. Select the **Unique** option if you want to indicate on the data entry form that this detail (data field on the form) needs to be filled in with a unique value. In other words, duplicate entries among recorded items won't be allowed in this data field.

If you select the Unique option, the Required option (below) is automatically selected as well. This is because a data field that asks for a unique value is considered a required field by default.

6. Select the **Required** option if you want to indicate on the data entry form that this detail (data field) must be filled in with valid data. A required field is indicated by the red "i" icon on a data entry form. A required data field does not necessarily have to be filled in with unique data.
7. If you selected the String type, you must specify the maximum number of characters allowed in the string by entering a numerical value in the **Length** field. The valid range is from 1 to 4,000 characters for English and other European languages (the range is from 1 to 2,000 characters for supported double-byte Asian languages). This field is required for a string and is not available for any other information type.
8. Again, if you selected the String type, you can enter a required format or syntax in the **Input Mask** field. This field only applies to strings and is optional.

The input mask indicates a required format when entering data for this detail on a data entry form. For example, if the detail is a serial number that must conform to a certain format such as "abc-123456" you would enter an input mask like this: aaa-#####, where lower-case "a" represents any letter, the hyphen is a literal character, and the pound character (#) represents a number. For the actual character a, use the /a exception. For the actual pound character (#), use the /# exception. This mask appears on the data entry form so the user knows how to enter data for the field.

Note: Only the alphanumeric characters a-z, A-Z, and 0-9 are supported when filling in a string detail on a data entry form whose required syntax is specified by an input mask; extended characters and double-byte characters are not supported.

9. If you want to specify a value that will automatically appear in this detail's data field on a data entry form, enter that value in the **Default Value** field. This option applies to all the information types and is not required. All default values on a form can be edited. (To enter a default date value, use the calendar control.)
10. If you want this detail to appear on the item list page for the type you're configuring, select the **Summary** option. This option is checked by default. If you clear the Summary option, this detail does not appear on the item's list page.
11. If you want to configure a controlled list of valid data entry values for this detail, select **Static List** type. A new dialog appears to the right that lets you add values to the static list. The values you add to this list will be available for this detail in a drop-down list on the data entry form.

To add values to the static list, simply enter a value in the **Add Values** text box and click the plus sign (+). To set a value as the default value (automatically appears in the detail's data field on a data entry form), select the value and then click **Set Default**. To remove a value, select it and click **Remove**.

12. If you want to use a global list type to define this detail, select **Global List** type. A new dialog appears to the right that lets you choose from the current global list types (see Managing global lists). The values that have been added to the database for the selected type will be available for this detail in a drop-down list on the data entry form.

Global lists contain general information that is standard throughout your organization, such as vendors, users, and locations. To use a global list type to define this detail, first select the subgroup that includes the global list type you want from the **Select Group** drop-down list, and then select the global list type from the **Select Type** drop-down list. (If you want to assign a default value to this detail (data field on the form), select a value from the **Select Default Value** drop-down list. Keep in mind that if no data has been entered into the database for that type yet, this list will be empty.)

13. When you're done configuring the settings and values for the detail, click **Return to form** to save the detail and return to the details summary page. Or, click **Cancel** to exit without saving the detail.
14. If you want to place the detail in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see Organizing details in sections.
15. **Important:** You must also click **Save Details** on the details summary page to save any details you've added or modified.

Rules for editing details

After a type has been saved, you can edit only some of the information fields for the details that define that type.

Remember that a type must have at least one detail, called the key detail. In addition to its key detail, a type can have any number of additional details that help define that type and help you track and manage your IT assets.

Non-editable fields

For both key and non-key details, AFTER the detail is saved you can't edit any of the following information fields on the Edit Detail page:

- Name
- Type
- Key
- Unique
- Required

Editable fields

Whether the other information fields can be edited is different for key and non-key details, as described below.

For key details:

For a key detail, the table below shows the fields on the Edit Detail page that can be edited, depending on the selected information type:

Information Type	Length	Input Mask	Default Value	Summary
String	Yes	Yes	Yes	No
Integer	No	No	Yes	No
Date	No	No	Yes	No
Decimal	No	No	Yes	No
Alert Date	No	No	Yes	No

For non-key details:

For a non-key detail, the table below shows the fields on the Edit Detail page that can be edited, depending on the selected information type:

Information Type	Length	Input Mask	Default Value	Summary	Static List Values	Global List Default Value
Integer	No	No	Yes	Yes	No	No
String	Yes	Yes	Yes	Yes	No	No
Date	No	No	Yes	Yes	No	No
Decimal	No	No	Yes	Yes	No	No
Alert Date	No	No	Yes	Yes	No	No
Static List	No	No	Yes	Yes	Yes	No

Global List	No	No	No	Yes	No	Yes
--------------------	----	----	----	-----	----	-----

Adding detail tables

Use this page to add a detail table to the selected type. A detail table consists of one or more details and appears as an expandable table data field on a data entry form, each detail represented by a separate column in the table.

On a data entry form, an Expand/Collapse icon next to a data field name (without a text box) identifies a detail table. In contrast, an Expand/Collapse icon next to a data field with a text box identifies a global list type.

One example of a table data field on a form is a service history table, that consists of details such as cost, service date, technician, vendor, and so on.

When filling in a form, users can add as many entries as they like into a table data field by clicking the **Expand** icon, clicking the **Add** link, filling in the fields, and then clicking the **Add to table** link. This process can be repeated as many times as you want to add entries to the table.

Some predefined types (and their associated data entry forms) include predefined detail tables. You can also create your own custom tables and add them to types. A table is specific to the type to which it was added (i.e., it can't be shared with other types).

To add a detail table to a type

1. From any details summary page, click **Add table**.
2. In the **Details for** field, enter a unique name for the table.
3. Click **Add detail** to define an individual detail that appears as a column in the table. A table must include at least one detail (data field on the form).
4. You can also click **Choose template** to select from a list of existing detail templates that will add several details at once to the table. Each detail appears as a single column in the table.

Details in a table display in the order in which they were entered and can't be moved.

5. When you're done configuring the table, click **Save Details** to save the table. The new table appears in the details list as a Table type. Details display in the list in alphabetical order unless they belong to a specific section.
6. If you want to place the detail table in a specific section on the form, click **Manage sections**, select the section in which you want the table to appear, click **Edit**, and move the table to the **Current Details** box. For more information, see Organizing details in sections.
7. **Important:** Click **Save Details** again (this time from the details summary page) in order to save the changes you've made.

Once a table is configured, you can:

- Edit a table's details by clicking the pencil icon.
- Delete an existing table by clicking the X icon.

Managing detail templates

Use the Detail Templates page to view, create, edit, and delete detail templates. Detail templates are sets or groups of details that make it easy and convenient to add several details at once to a type.

Note: You add a detail template to a type from the type's details summary page, not from the Detail Template page. You can also add a detail template to a table from the table's details summary page.

Asset Manager includes a few predefined detail templates, and lets you create as many new detail templates as you want in order to facilitate the creation of custom types and detail tables.

To create a detail template

1. From the Asset Management menu in the Web console, click **Detail templates**.
2. Click **Add template**.
3. Enter a unique name for the template in the **Details for** field.
4. Add as many details as you want to the template by clicking **Add detail**.
5. When you're done adding details to the template, click **Save Details** to save the template and return to the templates list.

Note: When you add a details template to a type, all of the details contained in that template are added as individual details, not grouped as a template. In other words, a details summary list does not indicate in any way whether details came from a template.

To edit a detail template, click the pencil icon next to the template name.

To delete a detail template, click the X icon next to the template name.

To rename a detail template, click the text field icon. (You can rename all of the predefined types with the exception of the computer and software types. You can also rename your own custom types.)

Adding detail templates

Detail templates are sets or groups of details you can use to add several details at once. You can add detail templates to a type's details summary list or to a detail table.

Detail templates are not specific to a type or table; you can view and add currently available templates from any details summary page.

To add a detail template

1. From any details summary page (for either a type or a table), click **Choose template**. All of the existing detail templates appear in a list, and show all of the details in each template.
2. Find the template you want to add to the details summary, and click **Add template**.

All of the details contained in the template you just added appear as individual details in the details summary. They're not grouped or identified as coming from a template.

3. If you want to place any of the newly added details in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see Organizing details in sections.
4. **Important:** You must also click **Save Details** on the Detail for... page to save any details you've configured.

Using an item list

The item list page provides a summary view of all the items recorded in the database for the type named at the top of the page. To see a type's item list page, click the name of the type on the Assets, Contracts, Invoices, Projects, or Global Lists pages.

The information that displays in the columned table on an item list page is determined by the details that have the Summary option checked. In other words, if Summary is checked then the detail appears on the item list page. You can click the column headings to sort by that detail (data field).

To add items to the database, click the **Add** link, and then fill in the data entry form. For more information, see Adding items.

To edit an item's recorded data, click its **pencil icon**, and then enter new data. When editing, the item's data entry form includes a few extra options. For more information, see Editing an item.

To delete an item from the list (and from the database), click its **pencil icon**, and then click **Delete**.

Additional item list tasks

From an item list page, you can also perform the following tasks:

- Associate items with other items and related information.
- Import data for items of the selected type.
- Export data for items of the selected type.

From the item list page for two asset types, computer and software, you can also:

- Update designated linked details (data fields) with scanned inventory and SLM information from the core database. For more information, see Working with computer assets and Working with software assets.

Adding items to the database

This page is the data entry form for the type named at the top of the page. Asset Manager includes several predefined asset, contract, invoice, project, and global list types, and provides the ability for you to create as many custom types in each of those categories as you like.

When you enter and save the information on a data entry form, the item is recorded in the database.

A slightly different version of this page appears when you're editing an item. For more information, see [Editing an item](#) below.

The contents and layout of a data entry form are defined by the type's details and sections. For more information, see [Using the details summary](#) and [Organizing details in sections](#).

Adding assets—and other important information such as contracts, users, and projects—to the database is *the* central task of someone who wants to gain all the benefits of proactive asset management for their organization. Asset Manager provides the tools necessary to configure asset types and the detail elements that define them, to track that data, and ultimately to analyze and share that data through custom asset reports. However, the benefits of asset management to your business, in real terms, depends on the recorded data itself. If most of the fields in a well-designed and thorough data entry form are left blank, there is very little to track, and running reports will be of minimal value. The recorded data is the key, and hence, data entry should be considered the most important step in implementing an effective asset management solution.

Although the information asked for on data entry forms can vary, the process of adding data is the same, as described below:

To add an item to the database

1. From any item list (accessed by clicking the name of a type on either the Assets, Contracts, Invoices, or Projects page), click **Add**. Or, you can access the same page by clicking the plus sign (+) **Add** link next to the item type.

Note: You can expand or collapse the sections of a form by clicking the section name. Also, refer to the Legend at the top of the form to understand the icons next to certain data fields. Detail icons are explained in [Understanding the detail icons](#).

2. Fill in the data fields. When adding or editing a detail, you can only enter data compatible with the field type (i.e., only an integer in an integer field, a text string in a string field, a date in a date field, etc.).
3. To save the item and continue adding more items, click **Save and add another**.
4. To save the item and return to the item list, click **Save and return to list**.

The new item appears in the item list.

Editing an item

If you're editing an item that has already been added to the database, this page displays the following additional options:

- **Associate items:** Opens the Associate items page where you can create associations between the selected item and other items recorded in the database.

- **Delete:** Removes the item from the item list and from the database. When you delete an item, any association to or from the item is also removed. This data can't be retrieved unless you've exported it beforehand to a CSV file.
- **Print preview:** Opens a print-friendly version of this page in a separate window that can be printed from the browser.
- **Last edited by:** Lets you view (at the bottom of the page) the user who most recently modified this item, their core server, and the time.

Using asset alert dates

Asset Manager includes an alerting feature that lets you create and enable alert dates for any of the IT assets you add to your database. Asset alerting uses the standard LANDesk Alert Management System (AMS) and its accompanying Alert Settings tool (**Configure | Alert Settings**) where you can configure the precise alert action you want to notify you when an asset's specified alert date is reached.

About the Alert Management System (AMS)

This section describes how to create and enable alert dates for the assets you record and track with Asset Manager. For more detailed and complete information on the Alert Settings tool, see [Using alerts](#).

Alert dates are a convenient way for you to be automatically notified when a predefined deadline for a particular asset item is reached. For example, you can set an alert date to notify you when a lease expires, a contract needs to be renewed, a project milestone is scheduled, or when a computer should be upgraded. You can use alert dates for any purpose to help remind you of important asset-related tasks that need to be performed by a certain date.

In order to use asset alert dates, an asset must first have an alert date detail as part of its type definition. You can use existing alert date details that are already included with most of the predefined asset types, or you can create your own new alert date details. Then, when adding items of that type to the database by filling out its data entry form, the alert date detail must be enabled and a date specified. You also need to decide how you'll be notified by AMS by configuring the alert action in Alert Settings.

Important: Notification actually occurs during the next scheduled Inventory Service Alert Check AFTER the specified alert date is passed.

To learn more about each of these steps, read the sections below:

- [Creating alert date details](#)
- [Enabling and specifying alert dates](#)
- [Configuring the asset alert in Alert Settings](#)

Creating alert date details

Most of the predefined asset types have an alert date detail, but not all. You can create additional alert date details for any of the predefined asset types. For new custom types that you create, you can also add alert date details. A custom type's key detail can be an alert date. An asset can have more than one alert date defined.

Alert date details are listed with all other details on a type's details summary page. They appear as data fields on the type's data entry form.

To create an alert date detail

1. From any Asset Manager type page (Assets, Contracts, Invoices, Projects, Global Lists), click the pencil icon next to the type that you want to create an alert date detail for. The type's details summary page displays.
2. Click the **Add detail** link.
3. In the **Name** field, enter a unique name for the alert date detail.
4. From the **Type** drop-down list, select **Alert Date**.
5. The **Key** option is available only if you're creating a new custom type. For more information, see [Creating new types](#).

6. Select the **Unique** option if you want to indicate on the data entry form that this detail (data field on the form) needs to be filled in with a unique value. In other words, duplicate entries among recorded items won't be allowed in this data field.

If you select the Unique option, the Required option (below) is automatically selected as well. This is because a data field that asks for a unique value is considered a required field by default.

7. Select the **Required** option if you want to indicate on the data entry form that this detail (data field) must be filled in with valid data. A required field is indicated by the red "i" icon on a data entry form. A required data field does not necessarily have to be filled in with unique data.
8. If you want to specify a date that will automatically appear in the alert date's data field on the data entry form, enter that value in the **Default Value** field. Click the calendar button, and then select the date you want in the calendar window.

You don't have to specify a default value, and any default value can be edited on a data entry form. If you specify a default value, the alert date data field will be enabled on the data entry form.

9. If you want this detail to appear on the item list page for the type you're configuring, select the **Summary** option. This option is checked by default. If you clear the Summary option, this detail does not appear on the item's list page.
10. When you're done configuring the settings and values for the detail, click **Return to form** to save the detail and return to the details summary page. Or, click **Cancel** to exit without saving the detail.
11. The new alert date detail appears on the details summary page in alphabetical order with all the other details.
12. If you want to place the detail in a specific section on the form, click **Manage sections**, select the section in which you want the detail to appear, click **Edit**, and move the detail to the **Current Details** box. For more information, see Organizing details in sections.
13. **Important:** You must also click **Save Details** on the details summary page to save any details you've added or modified.

Your alert date detail has been added to the type. The next time you add an item of this type by filling out its data entry form, you can enable the alert date data field, and then specify the date you want to be notified.

Enabling and specifying alert dates

As stated previously, alert dates (without a specified default value) are disabled by default. If you want to set an alert date for an item you're adding to the database, you must enable the alert date field on the asset's data entry form and then select the date.

To enable and specify an alert date for an item

1. From any item list (accessed by clicking the name of a type on either the Assets, Contracts, Invoices, or Projects page), click **Add**. Or, you can access the same page by clicking the plus sign (+) **Add** link next to the item type.
2. Fill in the required data fields.
3. For any alert dates you want to enable, clear the **Disable Alerts** check box. (Alert dates with a default value are already enabled. You can select a different date if you prefer, or you can disable the alert date.)

4. Click the calendar control button, and then select the date for which you want to be notified.

Important: Notification actually occurs during the next scheduled Inventory Service Alert Check AFTER the specified alert date is passed, by the action specified in Alert Settings.

5. To save the item and continue adding more items, click **Save and add another**.
6. To save the item and return to the item list, click **Save and return to list**.

The new item appears in the item list, with its alert date enabled.

Note: You can enable and/or disable alert dates, and modify the specified date, for any item that has already been added to an item list by clicking its pencil icon and making the changes you want.

Configuring the asset alert in Alert Settings

For assets that are being tracked by Asset Manager, the only valid alert event or condition that can be used to trigger an alert is a date (i.e., a specified date being reached). However, the asset date alert is only one of many alerts offered for various tools and services.

As with other alerts, you need to configure the notification method or action for the asset alert in Alert Settings (**Configure | Alert Settings**). The alert you need to configure is called "Asset alert date has been reached." This alert is located under the **LANDesk Inventory Server** object.

Available alert actions include: broadcast messages, Internet mail, SNMP trap, event log, and more.

For step-by-step instructions on how to configure each of these alert actions, see Configuring alert actions.

Adding the description field to an Internet mail action

If you choose to be notified via the Internet mail method, you must manually add and define the Description field to the alert message when configuring the alert action. The purpose of this field is to provide the recipient of the alert message with helpful information regarding the type, nature, and source of the alert. You can enter any text you want.

To define the Description field for the Internet mail alert action

1. At the console, click **Configure | Alert Settings**.
2. Open the **LANDesk Inventory Server** object.
3. Right-click **Asset alert date**, and then click **Configure**.
4. Select **Send Internet Mail**, and then click **Next**.
5. Select the core server you want to be notified, and then click **Next**.
6. Fill in the address, subject line, and SMTP mail server fields, and then click **Next**.
7. Move the **Description** parameter from the Alert Parameters list to the Alert Message list.
8. Enter any text you want in the **Description** field, and then click **Finish**.

Associating items

This page allows you to view, create, and delete associations between the item named on this page and any other item recorded in the database.

Through associations, you can establish and track relationships between any of your fixed assets and their supporting items such as contracts, locations, users, projects, and so on. For example, you may want to associate printers with their lease agreement contract; or PDAs with their users; or phones with their users, locations, and service contracts; and so forth. Associations provide another level of asset management.

Creating associations:

You can create associations only from an actual item page, not from the item list page.

Associations exist between actual items in the database, not between item types. Associations are bidirectional. In other words, if you create an association from a printer to a contract, the same association also exists from the contract to the printer in that specific contract's page.

You can associate the following item types with each other:

- Assets
- Contracts
- Invoices
- Projects

To create an association

1. From any item page, click **Associate Items**. (This is also the way to view an item's associations.)

Note: The Associated Items page refers to the selected item by its key detail.

2. Use the **Search** tool to locate items that you want to associate with the selected item. From the search results list, check the items you want to associate, and then click **Add to list**.
3. Click **Save** to save the associations and return to the item page.
4. Click **Cancel** to exit without saving.

To delete an association, click the X icon next to the association in the list. Deleting an item also removes all of its associations from the database.

Associated item information can be included in Asset Manager reports.

Importing items

Asset Manager provides the ability to import items for asset, contract, invoice, project and global list types. For example, if you have information for all your printers in a single spreadsheet, you could import printer data into the item list for the printer asset type. Importing and exporting lets you use asset management-specific data with other data tracking, database, and reporting tools.

Because you're importing items of a particular type, the **Import** link is only available on a type's item list page.

Required rights

In order to import and export items, a user must have either the Asset Configuration right or the Asset Data Entry right.

Supported file formats

Asset Manager's import and export feature supports both CSV (comma-separated value) as well as XML formatted files. You import data from a CSV or an XML file into an existing type. These file formats are compatible with other data management tools such as Microsoft SQL Server, Oracle, Microsoft Access, and Microsoft Excel.

Understanding the structure of the import file

The file you want to import must be organized in such a way as to accommodate all the details (data fields) used to define the type.

Each line in the import file represents a single item and therefore corresponds to an item row on the item list page. Furthermore, each line must contain the data for that individual item, separated by commas. Each comma-separated value corresponds to a column on the item list page. A line must include a value for every detail in the type. For example, if the type is defined by ten details, then each line in the import file must have ten values (a value can be empty as long as it's separated by commas). Furthermore, the data in each value must match the data type specified for that data field (i.e., integer, string, date, etc.), or the import fails.

It is a requirement that the first line of the import file contain the names of the details (that match the column headings on an item list page), separated by commas.

It might be helpful to envision the import file as basically being in the same format and layout as an item list page—a table listing where each column represents a detail and each line represents an individual item.

Importing items

To import items into an existing type

1. From the Assets, Contracts, Invoices, Projects, or Global Lists page, click the name of the item type you want to import items into.
2. On the item list page, click **Import**.
3. Enter the full path, including the filename, to the file you want to import in the **File path** field. You can click **Browse** to locate and select the file you want to import.
4. Click the **Valid column names** link to see a list of all the details used to define the selected type. A details summary window opens showing all of the type's details by name and other characteristics in a column list.

Important: Your import file's structure and contents must be compatible with the columns in this list (each column representing a detail). For more information on the correct structure of an import file, see Understanding the structure of the import file above.

5. To ignore duplicate data, click **Ignore**. Or, to update duplicate data, click **Update**.

Duplicate data is identified as such by the value of an item's key detail. If two items have the same value for their key detail, both items in their entirety (i.e., their key detail and any other details) are considered duplicate data. You can choose what the import procedure does with any occurrences of duplicate data like this with the **Duplicate handling** feature, as described below:

If you click **Ignore**, any item in the import file whose key detail value is the same as the key detail value of an item that already exists in the database is NOT imported. The item in the import file is ignored and the existing item is preserved.

If you click **Update**, any item in the import file whose key detail value is the same as the key detail value of an item that already exists in the database IS imported. The item in the import file replaces the existing one.

6. Click **Import now**.

If the import file is formatted correctly, the data is added to the database and the items appear on the item list page.

Exporting items

Asset Manager provides the ability to export data for asset, contract, invoice, project, and global list types. Importing and exporting lets you use asset management-specific data with other data tracking, database, and reporting tools.

Because you're exporting items of a particular type, the **Export** link is only available on a type's item list page.

Required rights

In order to import and export items, a user must have either the Asset Configuration right or the Asset Data Entry right.

When you export a type, all of the items currently recorded in the database for that specific type are exported. However, you can customize the data to be included in the export file by selecting which of the type's details you want exported. The selected details will be exported for all the items currently recorded in the database. You can also save a customized list of selected details as an export configuration for future use. Export configurations are specific to the type for which they are created.

Supported file formats

Data can be exported as either a CSV (comma-separated value) formatted file or as an XML formatted file. These file formats are compatible with other data management tools such as Microsoft SQL Server, Oracle, Microsoft Access, and Microsoft Excel.

Understanding the structure of the export file

As stated in the Importing items section, the structure or layout of this exported file essentially matches the layout of an item list page, where each line in the file represents a distinct item record, and each comma-separated value in a line represents a detail (data field) for that item.

Export file names

All items for the selected type are exported in a single file (typename.csv). If the type has table data fields, then each table is exported as a separate file (typename-tablename.csv).

Exporting items

To export items

1. From the Assets, Contracts, Invoices, Projects, or Global Lists page, click the name of the item type you want to export.
2. On the item list page, click **Export**.
3. To use an existing export configuration, select it from the **Configurations** drop-down list.

Or, to manually specify the data you want included in the export file, clear the details you don't want exported. All details are checked by default.

If you want to save your selected details as a new export configuration for this type, enter a name in the **Configurations Name** field, and then click **Save**. The export configuration is added to the drop-down list and can be used at any time by this specific type.

4. Click **Export now**. The Export window opens displaying the files (and formats) that can be exported. You can export one or both of a file's two formats: CSV and XML.

Note on exporting table details

If you're exporting one or more table details for the type, each table detail must be exported as a separate file represented in the Export window by a unique file whose name corresponds to the table name.

5. Click the file you want to export.
6. At the browser's File Download dialog, click **Save**, choose a destination on the local machine, and then click **Save** again.
7. At the Download Complete dialog, click **Close**.
8. You can continue saving other export files from the Export window, and simply click **Close Window** when you're finished.

Using Asset Manager reports

Asset Manager includes a reporting tool that lets you collect and analyze the asset management data you've entered into the database.

The reporting tool includes several predefined asset management-specific reports that you can use to analyze the data you've entered for assets, contracts, invoices, and projects. These predefined reports provide examples of how you create and configure your own custom reports.

To view and edit a report's configuration, click the pencil icon.

To run a report and view the results, click the report name.

To delete a report, click the X icon.

Rights required to use asset reports

A user must have either the Asset Configuration right (which is equivalent to an administrator role for Asset Manager features and implies all Asset Manager rights) or the Reports right to be able to see and use the Reports link and features in Asset Manager. If a user has only the Asset Data Entry right, they won't even see the Reports link in the left navigation pane of the Web console. On the other hand, if a user has only the Reports right, they will see the Assets, Contracts, Invoices, Projects, and Global Lists links, but they can only browse those pages and can't create, edit, or delete any types, details, or actual items. For more information about the specific abilities provided by these asset management rights, see "Using role-based administration with Asset Manager."

Note: A user with only the Reports right does not count against your total number of user licenses for Asset Manager.

Rights are assigned to users by a LANDesk Administrator via the Users tool in the main console.

The Reports right for Asset Manager is the same Reports right that is used to provide access to the reporting tool in the console. Note that none of the Asset Manager reports are available in the main console's Reports tool (even for users with the Reports right). Asset Manager reports are only accessible via the Web console.

Using predefined Asset Manager reports

Asset Manager includes several predefined reports that generate information about the assets, contracts, invoices, projects, and related information recorded in the database. Some of the predefined asset reports are listed below. You can use these reports as examples or templates of what you can do with the Reports tool in Asset Manager.

- Ad-Hoc Projects Completed in Last 30 Days
- Ad-hoc Projects Started in Last 30 Days
- All Computers and Associated Items
- All Consulting Agreements
- All Leases and Associated Items
- All Mobile Phones
- All PDAs
- All Purchase Orders and Associated Items
- Computers by Cost Center Location
- Computers by Requested Date

- Computers Installed in Last 30 Days
- Leases by Business Code
- Leases by Cost Center Location
- Leases Expired in Last 30 Days
- Leases Expiring in Next 30 Days
- Purchase Orders by Cost Center Location
- Purchase Orders by Vendor
- Software by Cost Center Location
- Software by Request Date
- Software Installed in Last 30 Days

Creating and running custom reports

You can create, edit, run, and print your own custom reports.

There are three types of custom reports:

Date report: Provides information for a specific type's recorded items, grouped by one of its date details. For example, you could create a custom date report that gathers information about an asset based on its purchase date, or a contract based on its signature date. The results of a date report are determined by a specified timeframe (range of days) for the date detail. You can customize the additional details that are included in the report.

Summary report: Provides information for a specific type's recorded items, grouped by any one of its details. Summary reports always show a count number and at least one of the item's details. You can customize the additional details that are included in the report.

List report: Provides information for a specific type's recorded items, in a flat list. You can customize the additional details that are included in the report.

Use the procedure below to create and run a custom report:

To create and run a custom report

1. From the Reports page, click the **Add report** link for the type of report you want—date, summary, or list.
2. In the **Report name** field, enter a unique name for the report.
3. From the **Run report on** drop-down list, select whether to report on an asset, contract, invoice, or project type.
4. From the **Select type** drop-down list, select the specific type for whose recorded items you want to gather information. This list includes all the currently available types for the selected category.

If you're creating a **list report**, skip to step 7.

5. For a **date report**:

First, from the **Group by detail** drop-down list, select the date detail you want to base this report on, and under which the items in this report will be grouped. Or, select a global list type (in parentheses), and then select the date detail from its submenu. (The drop-down list includes the currently available *date* details for the selected type, plus any global list types whose date details the selected type uses.)

Then, in the **Timeframe** field, enter the number of days (before or after today) whose dates you want to include in this report. For example, 0 (zero) indicates today, -30 indicates 30 days before today (including today), and 30 or +30 indicates 30 days after today (including today). The date report will include all of the type's recorded items whose specified date value matches a date within this timeframe.

6. For a **summary report**:

First, from the **Group by detail** drop-down list, select the detail you want to base this report on, and under which the items in this report will be grouped. Or, select a global list type (in parentheses), and then select the detail from its submenu. (The drop-down list includes *all* the currently available details for the selected type, plus any global list types whose details the selected type uses.)

Then, if you want the summary report to include only the detail selected above and an item count, clear the **Details** check box. If you clear this option, the Shows columns and Related details options are dimmed and can't be selected. However, if you want to configure additional information to appear in the summary report, make sure **Details** is checked (the default setting), which allows you to select the other information options.

7. Specify the columns (that display details on an item's page) you want to include for each item in the report with the **Show columns** option. You can choose to include just the key detail, the summary details, or all details.
8. Specify additional information you want to include for each item in the report with the **Related details** option. You can choose to include none, table details, or associated items.
9. Click **Save and run** to save this report configuration and generate the report's results. A separate browser (pop-up) window opens and displays the report, which you can view and print.
10. Or, click **Save** to save the report configuration and return to the Reports page without running the report.

If you selected either of the two save options, the report is added to the alphabetical list on the Reports page.

As with predefined reports, you can view and edit a custom report configuration by clicking the pencil icon, and run a custom report by clicking the report name.

You can print a report from the report's pop-up window, according to the browser's Print settings.

Using Handheld Manager

LANDesk® Handheld Manager provides extensive inventory management and software distribution for handhelds. Unify desktop, server, and mobile device management in a single solution.

Handheld Manager provides:

- Asset management
- Software distribution
- Bandwidth throttling and checkpoint restart
- Automated update and device maintenance

Optimized for the low-speed, intermittent connections characteristic of handhelds, Handheld Manager integrates comprehensive handheld management with enterprise-level task control.

Handheld Manager provides handhelds with the same detailed inventory and software distribution capabilities that LANDesk provides for desktops, servers, and laptops. A lightweight inventory scanner catalogs detailed hardware and software attributes and stores them in the central inventory database. That enables robust license tracking, reporting, and change control, as well as easy targeting for software deployments.

Handheld Manager's seamless integration with LANDesk means you can manage handhelds right alongside your desktops and laptops. Use the same familiar querying tools to track inventory, and the same powerful task scheduler to distribute software. There's no need to learn specialized tools to support handheld devices.

Easily distribute software packages and updates to both wired and wireless Pocket PC devices using LANDesk's familiar task scheduler. This enables IT to establish standards and ensure that the right tools are available to your mobile workforce—wherever they may be at the moment—so they spend their time working, not configuring their handhelds.

Handheld Manager supports these features:

- Palm*: Inventory only
- Pocket PC*: Inventory, software distribution, and handheld file exchange
- Blackberry*/RIM: Inventory only

Note: This product installs with Management Suite automatically. It only needs to be activated.

Read this chapter for more information on:

- Installing Handheld Manager
- Using Handheld Manager
- Working with BlackBerry* devices

Installing Handheld Manager

Handheld Manager has these system requirements:

- LANDesk Management Suite 8.5 inventory and software distribution agents on host computers that handhelds are connected to (required for Palm handheld agent installation, optional for Pocket PC host computers)
- For Palm handhelds, Palm OS 4.0 or greater
- For Pocket PC handhelds, Windows Mobile* 2002 or 2003
- About 80 KB of memory on Pocket PC handhelds, about 25 KB of memory on Palm handhelds
- For BlackBerry handhelds, Java 3.6 or greater, and a BlackBerry Enterprise Server on your network

Installing Handheld Manager on handhelds

Handheld Manager Setup creates handheld client installation files on the core server. Handheld Manager supports two types of agent installations. Setup creates a Web share in this folder: `\Program Files\LANDesk\ManagementSuite\Handheld`. Software distribution uses this folder to store files that you have scheduled for distribution to Pocket PC handhelds.

- Pocket PC users can use a Web browser to directly run the installation .CAB file (`ldhm-815-mobile-2k-arm.cab`) from the LDLogon share on the core server. This is a “pull” installation. The URL would be `http://<servername.mycompany.com>/LDLogon/ldhm-815-mobile-2k-arm.CAB`. The “2k-arm” portion of the filename changes depending on the core server operating system version and the handheld processor type.
- Both Pocket PC and Palm users can receive client agents through a “push” installation. This method uses a standard software distribution script to deploy the Handheld Manager client agents to the handheld host computer. The next time the handheld synchronizes with that computer, it receives the handheld agent.

You can create a query that returns computers with handhelds attached to them. You can then use this query as the target for a client agent distribution script.

- For Palm handhelds, query on **PDA | Palm OS | Version**, and select 4.0 or greater.
- For Pocket PC handhelds, query on **PDA | Windows CE | Device Processor**, and select equals Arm. Handheld Manager only supports the Arm processor, and Arm support became available with Windows Mobile 2002.

To remotely install handheld client agents

1. From the Management Suite console, create a query for Pocket PC or Palm handhelds as described earlier.
2. Click **Tools | Distribution | Manage scripts**. Click the **My scripts** group, and click the **New distribution script** button.
3. Browse to the core server's LDLogon share and select the appropriate installer for the handheld platform you're distributing to.
For Pocket PC handhelds, select **ldhm client setup.exe**.
For Palm handhelds, select **ldscnpalm-8.1-5.exe**.
4. Finish the wizard. Click **Help** on a page if you need more information.
5. Schedule the script you just created, and either use the results of your handheld query or target host computers individually.

6. After the job runs successfully, the next time the handheld synchronizes with the targeted host computer, the host will install the Handheld Manager agents.

Understanding Pocket PC client agent installation

On Pocket PC push installations, Handheld Manager Setup copies a .CAB file to the computer that a Pocket PC synchronizes with. The contents of this .CAB are installed on the Pocket PC the next time it synchronizes. The .CAB contains these files:

- **setup.dll:** Handles the install/uninstall events and custom installation for the `wcetrigger.exe`. Upon successfully installing the handheld agent, it will call `wcetrigger.exe /I` to install the trigger. Before uninstalling the handheld agent, it will call `wcetrigger.exe /U` to uninstall the trigger.
- **wcescn.exe:** Inventory scanner. By default, the scanner runs once per day. The scanner places the scan file, `ldcescan.txt`, in the handheld's root folder (`\Program Files\LANDesk`).
- **wcetrigger.exe:** Launches programs in `ldlaunch.ini` when a network or desktop connection is established.
- **wcesdclnt.exe:** Distribution agent that communicates with the core server.
- **wcedwnld.dll:** Handles the file download.
- **ldlaunch.ini:** Text file that contains programs `wcetrigger.exe` should launch. By default, this file contains references to `wcesdclnt.exe` and `wcescn.exe`. It also includes the launch frequency and the next launch time.
- **ldcfg.txt:** Text file that contains the fully-qualified domain name for the core server.

These files are stored in the handheld's `\Program Files\LANDesk` folder. Handheld Manager stores temporary files in the `\Program Files\LANDesk\LDCache` subfolder. Temporary files are programs that are being distributed to a handheld but that haven't finished downloading. Once a program installs (or if it fails to install successfully), Handheld Manager deletes the temporary file.

Understanding Palm client agent installation

Palm handhelds only support inventory scans. Unlike Pocket PC handhelds, Palm handhelds don't communicate with the core server directly. Palm handhelds have a small inventory scanner program on them that uses a HotSync conduit to pass inventory scan data to the computer the Palm handheld HotSyncs with. The Palm inventory scanner runs on each HotSync. The Management Suite inventory scanner includes the handheld inventory scan file when the host computer sends an inventory scan to the core server.

Handheld Manager Setup makes these changes to computers hosting Palm handhelds:

- Setup installs a HotSync conduit, `ScannerConduit.dll`. When the Palm device synchronizes with the desktop, the desktop inventory scanner uploads the scan file to the core server, where the Inventory service adds them to the database.
- Setup configures the Palm inventory scanner, `ldscanpalm.prc`, so that it gets installed to the handheld on the next HotSync.

Once `ldscanpalm.prc` is installed, it stores inventory data in `palmscan.scn`. During each HotSync, the Handheld Manager conduit copies this file to the host computer's `C:\Program Files\LANDesk\LDClient\Palm\Transfer` folder. The desktop inventory scanner looks here for scan files to send to the core server. This file gets overwritten each HotSync.

Using Handheld Manager

Once the agents are on handhelds, you can:

- Query handheld inventory data
- Distribute programs to Pocket PC handhelds
- Transfer files to and from Pocket PC handhelds

Querying for handheld inventory data

The Management Suite inventory scanner stores handheld inventory information in two places:

- Under the PDA attribute: This attribute contains handheld inventory data from computers that host handhelds. This information is limited, since it doesn't come directly from the handheld.
- In the standard device attributes: The handheld inventory scanners put inventory data in the normal device attributes. For querying on this data, use the same attributes you would use to query for computer data. Don't look for handheld inventory scanner data under the PDA attribute.

Changing the Pocket PC inventory scan frequency

Each time a Pocket PC handheld connects to the network, `wcetrigger.exe` checks `ldlaunch.ini` in the `\Program Files\landesk` folder on the handheld. This file contains one application (and path) per line with its run-time parameters that will get executed by the `wcetrigger.exe`. The line containing `wcescn.exe` controls the inventory scanner, and the line containing `wcesdcInt.exe` controls the software distribution agent.

The file format is as follows:

```
\Program Files\landesk\wcescn.exe|daily|6/4/2004  
\Program Files\landesk\wcesdcInt.exe|3|6/4/2004 14:00
```

Each line is split by the pipe (|) character. The first element is the path and name of the executable. The second is one of the following keywords: hourly, daily, [numeric value].

If the keyword is hourly or daily, the third element is the next runtime, either the date and time or just the date. If the keyword is a numeric value, indicating the number of hours between runs, then the third element is the next runtime.

For instance, in the example above the `wcescn.exe` file would be run every day (regardless of the time). The next runtime would be the first time it connects to a network on 6/4/2004. The `wcesdcInt.exe` would be run every 3 hours, with the next runtime being at 2:00 PM. After each execution, the file's runtime is updated.

Only whole numbers are supported as a modifier hour. The execution time must include a date, but a time is optional. The time supports AM/PM or military.

You can update `ldlaunch.ini` handhelds using Handheld Manager's file exchange feature.

Distributing programs to Pocket PC handhelds

Handheld Manager software distribution to Pocket PC handhelds supports these Management Suite distribution features:

- **Checkpoint restart:** Restarts interrupted distribution downloads at the point the download was interrupted.
- **Bandwidth throttling:** Controls the file transfer speed to limit the amount of network and handheld bandwidth used.
- **Packet sleep options:** Adjusts the interval between distribution network packets. Higher intervals slow down the packet rate, using less bandwidth.
- **Feedback options:** For .CAB installations, you can select whether files install silently or with whatever UI the .CAB was configured to show (typically a progress bar).

All programs you want to install on Pocket PC handhelds must be in .CAB or .EXE format. After the file is on the handheld, Handheld Manager executes the .CAB or .EXE file.

The \Program Files\LANDesk\Management Suite\Handheld folder on the core server is a read-only Web share that any client can access. When you schedule a handheld distribution job in the Management Suite console, the console copies programs you're distributing to this share. The handheld distribution agent will retrieve the program from this share on the core server. You can't host files you want distributed to handhelds in a different location.

Create a handheld distribution job from **Tools | Distribution | Scheduled tasks** in the Management Suite console. There's a **Schedule handheld task** button in this window that launches the handheld script wizard.

Before you can distribute software to handhelds, they must have the Handheld Manager client agents on them. Once they return an inventory scan, you'll be able to make Pocket PC handhelds distribution job targets. Don't target the handheld host computer for handheld distribution jobs. You only need to target the host computer for initial handheld agent installation.

When you schedule a handheld distribution job, the job status briefly reports "Working," and the status changes to "Available for Pull." The next time the handheld connects to the network, wcesdcint.exe will check with the core server for available jobs, see the job you have scheduled, and start downloading the program. By default, wcesdcint.exe runs once per hour.

When the job finishes, the job status changes to "Successful."

To distribute software to a Pocket PC handheld

1. Copy the program you want to install to a Web share.
2. Click **Tools | Distribution | Scheduled tasks**, and click the **Schedule handheld task** button. Browse to the program you want to install and click **Next**.
3. Enter a **Script name** and click **Next**.
4. Adjust the download options you want and click **Next**.
5. Select whether you want the package to install silently or not and click **Next**.
6. Finish the wizard.
7. From the network view, drag handheld clients that you want to receive the package to the task you created in the **Scheduled tasks** window.
8. From the task's shortcut menu, click **Properties** and configure the task. Once the start time arrives, the job status will change to **Available for Pull**, indicating that the file has been made available to the handheld the next time the handheld distribution agent runs (the default is once an hour). You can force the agent to run by running wcesdcint.exe on the handheld.

Understanding distribution options

When you create a handheld distribution script, the wizard includes a **Download options** page that has the bandwidth throttling options below. The defaults normally work fine since handheld packages tend to be small. If you want to adjust the bandwidth used, adjust these options:

- **Dynamic bandwidth throttling:** Specifies that the network traffic a client creates has priority over distribution traffic. If you select this option and leave the **Minimum available bandwidth percentage** at 0, once the client initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops.
This option forces a full download of the file into the client's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted.
- **Minimum available bandwidth percentage to use on client:** Specifies how much dynamic bandwidth throttling to apply. You can enter values of up to 50 percent of the total network bandwidth available to the client. For example, if there were one other application consuming network bandwidth on the client during a distribution and you set the bandwidth percentage to 50 percent, the distribution job would take 50 percent and the client application would take 50 percent. In practice, this percentage is variable because the operating system automatically allocates much of the network bandwidth depending on the number of applications needing bandwidth and their priority.
- **Delay between packets (source):** Specifies the delay between the package source and client destination. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

Transferring files to and from Pocket PC handhelds

Handheld Manager's file exchange feature lets you place files on Pocket PC handhelds or transfer files from Pocket PC handhelds to the core server.

Sending files to handhelds

Before sending files to handhelds, Handheld Manager bundles them in a standard .CAB format, which then gets installed on the handheld. The .CAB includes the file and the path on the handheld the file should be installed to. Any existing files in the same path with the same name are overwritten.

Sending files to handhelds requires two steps:

- Create a .CAB file containing the files you want sent
- Distribute the .CAB file to the handhelds that need it

To create a .CAB

1. Click **Tools | Handheld | Handheld file exchange**.
2. In the Handheld File Exchange window, double-click **Create handheld CABs**.
3. Enter the .CAB name.
4. Select a file to include by browsing for it or typing in the path and filename.
5. Enter the destination path on the handheld. Don't include the filename.
6. Click the **Add** button to add it to the .CAB.
7. Repeat steps 4-6 for each file you want the .CAB to install.
8. Click **Create** when you're done adding files to the .CAB.

Once you've created a .CAB, distribute it as described in "Distributing programs to Pocket PC handhelds".

Retrieving files from handhelds

Handheld Manager's file exchange feature also allows you to retrieve files from Pocket PC handhelds. The **Files to backup from handheld** dialog manages the file list. There is only one backup list and it applies to all Pocket PC handhelds. Any changes you make are immediately applied once you click **Apply** or **OK**. Handhelds send the files you specified to the core server when they do their next scheduled inventory scan.

When you use handheld file exchange to retrieve files from the handheld, they're copied to this location on the core server:

```
\Program Files\LANDesk\ManagementSuite\hhfilex\<letter of
alphabet>\<login name>\<GUID>
```

Handheld Manager creates an alphabetical directory structure under the ..\hhfilex folder. Each letter contains a subfolder matching the login name for the user logged in when the device uploaded files. If the login name isn't available, there's a <GUID> folder that contains folders named with the handheld's Windows GUID (Globally Unique Identifier).

When saving handheld files on the core server, Handheld Manager resets the file date and time to match the time it was created on the core server. By default, Handheld Manager will keep backup versions of files for three days. Backups are renamed with a .bak.0001, .bak.0002, .bak.0003, and so on extension. The most recent backup will have the .bak.0001 extension. Backup files are not deleted until there are 9999 of them, where the oldest gets deleted upon each new file being saved.

To retrieve files from handhelds

1. Click **Tools | Handheld | Handheld file exchange**.
2. In the Handheld File Exchange window, double-click **Handheld files to back up**.
3. To add a file, enter its path and filename on the handheld and click **Add**.
4. To remove an existing file, select it in the list and click **Remove**.
5. Change the delay and buffer size if necessary. These options control the amount of network bandwidth handhelds use to transfer files.
6. Click **OK** when you're done.

Working with BlackBerry devices

Handheld Manager can do inventory scans on BlackBerry devices that run Java 3.6 or later. The scanner reports the device type, version, OS, battery info, network connection, display type and resolution, installed software, and other data.

Handheld Manager's BlackBerry support requires that your network have a BlackBerry Enterprise Server (BES). The BES allows BlackBerry devices to communicate with the Management Suite core server.

The BlackBerry agent consists of three files in the pocketpccabs share on the core server:

- com_Landesk_LdBbScanner.cod
- com_Landesk_LdBbScanner.jad
- com_Landesk_LdBbScanner.alx

The easiest way to have clients install the scanner is to send them an e-mail such as the following:

Please click on the following link to install the LANDesk Inventory Scanner for BlackBerry/RIM devices:

`http://<coreserver>/pocketpccabs/com_Landesk_LdBbScanner.jad`

Once the scanner installs, open the LANDesk Inventory Scanner from the ribbon bar.

From the scanner's menu, select Configure Scanner and do the following:

Enter <your core server name> in the Core Server field. Enter your name in the Owner Name field. Save the changes when you're done.

You can also have users install the scanner from the BlackBerry Desktop Manager. Use the application loader and browse for \\coreserver\pocketpccabs\com_Landesk_LdBbScanner.alx. Finish the wizard to install the scanner.

Once users install the scanner, it appears in the device's ribbon bar. Users must enter the core server name for the scanner to work. The scanner can run without any other information, but having users fill in the Owner Name may help you identify scans more easily.

If users don't enter configuration information or the scanner can't contact the core server, the next time the scanner runs it will display the configuration screen and prompt for updated configuration information.

Scanned BlackBerry devices appear in the network view. Their device name is the BlackBerry 7-digit PIN. To preserve battery, the inventory scan does not run automatically. It must be manually run from the device.

Using LANDesk Inventory Manager

LANDesk Inventory Manager is a version of LANDesk Management Suite 8 that contains only these inventory-related features:

- Inventory scanning and inventory-related console features
- Custom data forms
- Software license monitoring
- Unmanaged device discovery
- Reports for the above features

The Inventory Manager installation on a core server contains all LANDesk Management Suite 8 components, but when you activate a core server with an account that is licensed for Inventory Manager, the non-Inventory Manager features aren't applicable or visible in the Management Suite and Web consoles.

If you're using Inventory Manager, refer to the sections that correspond to the list of features above. Typically, you can recognize the information that doesn't apply in each chapter because those sections refer to Management Suite features like software distribution and remote control that aren't part of Inventory Manager.

Appendix A: Additional inventory operations and troubleshooting

LANDesk uses an inventory scanner utility to gather hardware and software information for the devices on your network. For information on inventory scanner basics, see the Managing inventory and Managing reports chapters. This chapter provides additional information about inventory scanning, as well as some troubleshooting tips.

Read this chapter to learn about:

- Scanning custom information
- Specifying the software scanning interval and history
- Scanner command-line parameters
- Scanning standalone devices with a floppy disk
- Adding inventory records to the core database
- Adding BIOS text strings to the core database
- Creating MIF files
- Scanning NetWare servers
- Editing the LDAPPL3.TEMPLATE file
- Troubleshooting the inventory scanner

Scanning custom information

The Windows inventory scanner utility (for Windows 95/98 and Windows NT/2000/2003/XP) automatically scans the device's registry for custom information. When you configure a device, the following keys are installed into the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDESK\INVENTORY\CUSTOM_FIELDS
```

The inventory scanner always scans the registry for the Custom Fields key and picks up any information it finds under that key. It then enters the custom information into Custom fields in the core database. The information content doesn't matter. When you view this data in the console, it displays under Custom fields.

The inventory scanner reads two data types:

- REG_SZ
- REG_DWORD

Custom field subkeys

The inventory scanner doesn't scan for any subkeys below Custom fields.

Custom fields string length

ASCII character strings must be no longer than 255 characters. Multi-byte character set (MBCS) strings must be between 127 and 255 characters.

Configuring the scanner to scan registry keys

The inventory scanner can scan for registry keys you specify and add their values to the core database. This can be useful for customized software, asset information, or other information stored in the registry that you want to include in the core database.

To use registry key scanning, add a section at the very beginning of the LDAPPL3.TEMPLATE file with this format:

```
[Registry Info]
KEY=HKLM, Software\Intel\LANDesk, version, MyData - LANDesk - Version
```

Change the values after KEY= to match the registry key you're looking for. In the example above, notice that each registry key element is separated by commas.

When the inventory scanner retrieves the registry key data, you can view it in the path specified by the last parameter. Each level is separated by " - " (space dash space). To force the scanner to use a 64-bit hive, append 64 to the hive name. For example, HKLM64.

Specifying the software scanning interval and history

You can specify when to scan a device's software and how long to save the inventory changes history log on the core server. These intervals apply to every device.

Note: A device's *hardware* is scanned every time it boots and is connected to the network.

To specify the software scanning settings

1. In the console's network view, click **Configure | Services | Inventory | Software**.
2. Specify the frequency of software scanning.
3. Specify the number of days to save the history.

The core server and software scanning

This feature affects only devices. It doesn't affect the core server, which is always scanned daily.

Scheduling an inventory scan task

If the device is running the LANDesk agents, you can schedule a script that triggers an inventory scan on devices.

To schedule an inventory scan

1. Click **Tools | Distribution | Manage scripts**.
2. Click **All other scripts**.
3. From the inventoryscanner script's shortcut menu, click **Schedule**.
4. Configure task targets and the start time in the **Scheduled tasks** window.

The inventory scanner script is located in the \Program Files\LANDesk\ManagementSuite\Scripts directory. The script is a Windows .INI file that you can edit with any text editor. If you need to change the options or parameters within the script, open it and follow the instructions contained within it.

Scanner command-line parameters

You can add command-line parameters to the inventory scanner's (LDISCN32.EXE) shortcut properties to control how it functions.

The following table lists the scanner's command-line parameters:

Option	Description
/NTT=IP	Core server's IP address or DNS name and UDP port. For example, /NTT=123.123.123.123:5007 or /NTT=CORESERVER:5007. The OS/2 scan utility, LDISCAN2.EXE, and DOS scanner utility, LDISCAN.EXE, don't use this parameter.
/UDP	Scanner communicates via UDP instead of TCP.

	Combine this switch with /NTT=[IP].
/NTN=NetBIOS Lana number	NetBIOS Lana number the scanner should use.
/NOUI	Forces the scanner to run with no user interface.
/i=inifile	Provides the path (HTTP, UNC, or a drive letter) to the master LDAPPL3 file. LDISCN32.EXE also copies the LDAPPL3 file they find in this location to the device's local LDAPPL3.INI file. The scanners compare the date of the master LDAPPL3 with the local LDAPPL3.INI; if the dates don't match, the master file is copied locally.
/d=directory	Starts the software scan in the specified directory. By default, the scan starts in the root directory of each local hard drive.
/L	Sends the scan to the core server the device was configured from. When you use /L, the /NTT parameter isn't necessary.
/sync	Forces a full scan, including a complete software scan. Full scan files can be several megabytes in size.
/n	Doesn't search subdirectories.
/v	Verbose mode.
/Z=retry count	How many times the scanner tries to resend the scan.
/W=wait in seconds	Have the scanner wait the number of seconds specified before starting a scan.
/? or /h	Displays the command-line syntax help.
/s=servername	Specifies the core server to store the inventory data on.
/f	Forces a software scan regardless of the software scan interval set at the console. Specify /f- to disable a software scan regardless of the software scan interval set at the console.
/t=[path]filename	Copies the contents of the specified file to the core database. Use this option to enter inventory data from standalone devices or from separate inventory files.
/o=[path]filename	Writes inventory data to the specified output file.
/m	Creates a non-unicode LDISCAN.MIF file in the C:/DMI/DOS/MIFS directory. This file contains the inventory data discovered during the scan.
/muni	(LDISCN32.EXE only) Creates a unicode

LDISCAN.MIF file in the directory found in LDAPPL3.INI file's MIFPATH. This file contains the inventory data discovered during the scan.

Scanning standalone devices with a floppy disk

To scan a standalone device

1. Copy the proper inventory scanner utility and a software description file (usually LDAPPL3.INI) to a floppy disk. (You may also need to copy ELOGAPI.DLL, YGREP32.DLL, LOC16VC0.DLL, INV16.EXE, LOC32VC0.DLL, LTAPI.DLL, and LDISCN32.EXE.)
2. Run the scan with the /O= parameter specifying the path and filename of the output file.
3. At the command-line prompt, enter a unique name for the device. This name is saved in the LDISCAN.CFG file on the device's local drive. This name also appears in the Description field in the core database. For example:

```
ldiscn32.exe /f /v /o=c:\%computername%.scn
```

Adding inventory records to the core database

You can add inventory information from a standalone device or separate inventory files by running the inventory scanner from the operating system command line.

To add inventory records from a file to the core database

- Run the scan utility with the /S= , /T=, and either the /NTT or /NTI parameters.

Adding BIOS text strings to the core database

There is a section in the LDAPPL3.TEMPLATE file called [BIOS Info]. This section provides the capability to search for information inside the BIOS of a computer. You can add one or more entries to the [BIOS Info] section. These entries define new keys in the core database and provide parsing instructions to the inventory scanner. The parsing instructions identify where to look in the LDBIOS.TXT file for a specific string. Using these instructions, the inventory scanner populates the core database with the strings from the LDBIOS.TXT file.

The inventory scanner uses a parsing method to locate BIOS information. This allows you to search for information one or more lines away from a specified text string. Such a search would enable you to locate random letter and number combinations assigned to computer hardware.

Text strings in LDBIOS.TXT

During an inventory scan, the text strings available in the BIOS are exported to a text file called LDBIOS.TXT. This hidden file is stored in the same location as the LDISCAN.CFG file, which is by default the root of the C: drive. LDBIOS.TXT stores all of the strings that are created by the scanner. If you want to store this information in the database, you can store it as a configuration file by using the CFGFILES parameter in LDAPPL3.INI.

Sample of BIOS entries in the LDAPPL3.TEMPLATE file

Here is an example from the [BIOS Info] section in the LDDAPPL3.TEMPLATE file:

```
[BIOS Info]
StringLength=4
Key = BIOS - Manufacturer
Parameters = AllValues,FirstInstance
Value = AMI|American Megatrends::AMI::BIOS - AMI
Value = Copyright.*Dell::Dell::BIOS - Dell

[BIOS - AMI]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = (C).*\(AMI|American Megatrends\)

[BIOS - Dell]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Value = BIOS Version: \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = (C).*Dell|[Cc]opyright.*Dell
```

Understanding BIOS entries

Entries in the [BIOS Info] section consist of the following:

- **[Section name]:** Identifies a new component in the core database.
- **StringLength=:** Specifies the minimum length of the strings to search for.
- **Key=:** Identifies the class and attribute name of the information returned from searching the LDBIOS.TXT file.
- **Parameters=:** Specifies the search criteria that tells the scanner where and how to search for values associated with a specific key.
- **Value=:** Specifies the value that is searched for in the BIOS. A value has three main sections, each separated by a double colon character (::). The strings identified in the value entry are case-sensitive. All characters in the value, even spaces, are included in the search unless they are an operator.

Creating MIF files

If you need a MIF file that stores a device's inventory information, you can create one by running the appropriate scanner at the command line.

To create a unicode MIF file, use the /MUNI option. To create a non-unicode MIF file, use the /M option.

To create MIF files

- Enter this at a DOS prompt:

LDISCN32 /MUNI /V

Scanning NetWare servers

LANDesk uses LDISCAN.NLM to scan NetWare servers for hardware and software information. The command-line syntax for LDISCAN.NLM is:

```
LOAD LDISCAN[.NLM] INV_SERV=servername
NTI=IPX address FILE=path [TIME=#] [SCANNOW] [MIF]
```

The following table lists the command-line parameters that you can use with the NetWare scanner.

Option	Description
INV_SERV = serenade	Directs the results of the scan to the specified server. The specified server must be running the inventory service.
NTT = IP address	Gives the IP address of the core server to send the inventory information to.
FILE = path	Lists the path to the LDAPPL3.INI file.
TIME = #	Sets the time of day for the server hardware scan in whole hours. The clock is in military time, so 0 = midnight and 23 = 11 p.m. Configure software scans in Options Software Scanning. The default is 8 p.m.
SCANNOW	Forces an core server scan at the time the NM is loaded.
MIF	Creates the LDISCAN.MIF file for the core server. The .MIF file contains the inventory information gathered from the server.

To load LDISCAN.NLM on a NetWare server

- From the server console, enter the proper syntax at the LDISCAN.NLM command line.

For example, to scan a server daily and record its inventory data in the core database on "Server1," enter:

```
LOAD LDISCAN INV_SERV=SERVER1 TIMEWORK
NUMBER:NODE ADDRESS:SOCKET FILERS:MONEYCHANGER
```

To unload LDISCAN.NLM from a server, enter:

```
UNLOAD LDISCAN
```

Scheduling NetWare server scans

LDISCAN.NLM scans recur every day as specified by the TIME=# parameter. The TIME parameter is set in military time, so 0 is midnight and 23 is 11 p.m. The default is 8 p.m.

To change the time for server scans

- Add the TIME = # parameter to the load LDISCAN.NLM entry of LD_AUTO.NCF.

Editing the LDAPPL3.TEMPLATE file

Information relating specifically to the scanner's inventory parameters is contained in the LDAPPL3.TEMPLATE file. This template file works with the LDAPPL3 file to identify a device's software inventory.

You can edit the template file's [LANDesk Inventory] section to configure the parameters that determine how the scanner identifies software inventory. By default, LDAPPL3.TEMPLATE is located in this directory on the core server:

\Program Files\LANDesk\ManagementSuite\LDLogon

Use this table as a guide to help you edit the [LANDesk Inventory] section in a text editor.

Option	Description
Mode	<p>Determines how the scanner scans for software on devices. The default is Listed. Here are the settings:</p> <ul style="list-style-type: none"> • Listed: Records the files listed in LDAPPL3. • Unlisted: Records the names and dates of all files that have the extensions listed on the ScanExtensions line but that are not defined in the LDAPPL3. This mode helps discover unauthorized software on the network. • All: Discovers files with extensions listed on the ScanExtensions line.
Duplicate	Records multiple instances of files. Set the value to OFF to record only the first instance, or ON to record all detected instances. The default is ON.
ScanExtensions	Sets the file extensions (.EXE, .COM, .CFG, etc.) that will be scanned. Use a space to separate the file extensions. By default, only .EXEs are scanned.
Version	Is the version number of the LDAPPL3 file.
Revision	Is the revision number of the LDAPPL3 file; helps ensure future compatibility.
CfgFiles 1-4	<p>Records the date, time, file size, and contents of the specified files. You can leave out the drive letter (for example, c:) if you want to search all local drives. You can specify more than one file on each of the four lines, but the line length is limited to 80 characters.</p> <p>Separate path names on the same line by a space.</p> <p>The scanner compares the date and size of the current file with that of the previous scan. If the date and size don't match, the scan records the contents of the file as a new revision.</p>
ExcludeDir 1-3	Excludes specific directories from a scan. You can leave out the drive letter (for example, c:) if you want to exclude all local drives.

Enumeration must start at 1 and be continuous. You must end each line with "\".

MifPath	Specifies where MIF files are stored on a device's local drive. The default location is c:\DMI\DOS\MIFS.
UseDefaultVersion	If set to TRUE, the scanner reports a match when a file matches an exact filename and file size entry in LDAPPL3 on filename only (the version will be reported as EXISTS). This can cause some false positives for applications that share a common filename with an unknown application. In the as-delivered LDAPPL3.TEMPLATE file, this parameter is set FALSE; that is, only add an entry if the match is exact. If the parameter is missing, it defaults to TRUE.
SendExtraFileData	If set to TRUE, sends extra file data to the core server. The default is FALSE. This means that by default, only path, name, and version are entered into the core database.

To edit the LDAPPL3.TEMPLATE file

1. From your core server, go to the LDLogon directory and open LDAPPL3.TEMPLATE in Notepad or another text editor.
2. Scroll down to the parameter you're interested in updating and make your changes.
3. Save the file.
4. In the console, click **Tools | Reporting/Monitoring | Software License Monitoring**.
5. Click the **Make Available to Clients** toolbar button to make the most recent changes available to devices the next time they run an inventory scan if the /i scanner command line parameter is used on devices.

Troubleshooting the inventory scanner

This section describes common inventory scanner problems and possible solutions.

The inventory scanner hangs

- Make certain that you aren't including the old /DELL or /CPQ options on the command line. These options are no longer supported.
- Scan to a file using the /O= parameter. This may show a conflict with the network card or the network.

A device's hardware scans correctly, but its software doesn't

- Verify that the core database is configured to do a software scan now, and use the /f parameter to force a software scan.
- Scan to a file using the /O= parameter. This should list all of the software at the end of the file.
- Verify that the device is not trying to scan in a binary file in LDAPPL3.TEMPLATE's CfgFiles parameter.

The network view provides inventory data for only some devices

To view device information, ensure that your devices have been scanned into the core database. Devices appearing without information haven't been scanned into the core database.

To view a device's inventory data in the network view

1. Configure the device.
2. Scan the device into the core database.

For more information about configuring devices

Refer to Configuring device agents.

For more information about scanning devices

Refer to Managing inventory.

Specifying the number of days to keep inventory scans

By default, the core server keeps inventory scans for devices until you delete them. You can have the core delete inventory scans for devices if the device hasn't submitted a scan for the number of days you specify. Doing this can remove devices that are no longer on your network.

To specify the number of file revisions to keep in the core database

1. Click **Configure | Services | Inventory**.
2. Specify the number of days you want to keep inventory scans.
3. Click **OK**.

Appendix B: Additional OS deployment and profile migration information

The chapter provides supplemental information about LANDesk's OS imaging and profile migration capabilities.

Read this chapter to learn about:

- Creating an imaging boot disk
- Adding application package distributions to the end of an OSD script
- Using CSVIMPORT.EXE to import inventory data
- Creating custom computer names
- Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values
- Using images in mixed uniprocessor and multiprocessor environments
- Adding network adapter drivers
- Using the LANDesk imaging tool for DOS
- Using the LANDesk imaging tool for Windows

Additional OS deployment procedures

Creating an imaging boot disk

LANDesk OS deployment (OSD) includes a boot disk creation utility that allows you to easily create a disk you can use to boot devices into a managed state in LANDesk network. You can use this boot disk to continue OSD jobs on devices that do not have an operating system or that failed a job for some reason and are no longer bootable. Once you boot a device with this boot disk, you can schedule a job for it.

Note: A user must have administrator rights on the core server if they want to create an OSD boot disk (even if they already have the OS Deployment right).

Boot disks are associated with the core server where they were created. If you have multiple core servers, use a boot disk created from the core server you want the device to report to.

To create an imaging boot disk

1. Click **Tools | Distribution | Manage Scripts**.
2. In the Manage Scripts window, click the **Create Boot Floppy** toolbar button to open the Create Imaging Boot Disk dialog.
3. Insert a 1.44 MB diskette into the floppy disk drive and make sure the destination floppy drive is correct.

Note: All data on the diskette will be erased.

4. Select the network adapter you want this boot floppy to support. Each floppy can only support one adapter because of disk space limitations.
5. Click **Start**. The Status box indicates the progress of the disk creation.
6. When finished, click **Close** to exit the dialog.

Adding application package distributions to the end of an OSD script

You can easily make an Enhanced Software Distribution (ESWD) application package distribution part of your OS deployment script.

To add ESWD packages to an OS deployment script

1. Open your package script in the LANDesk/ManagementSuite/Scripts directory and copy the REMEXECx= package distribution lines.
2. Edit your script by right-clicking it in the Manage Scripts window and clicking **Advanced edit**.
3. Paste the ESW REMEXEC commands at the bottom of your script, changing the REMEXEC numbering so that the numbers are sequential.
4. Insert a line before the ESWD lines you pasted in for LDSLEEP, similar to below. This allows time for the OS to finish booting before starting the package installation.

```
REMECECxx=LDSLEEP.EXE 120
```

Replace xx with a unique sequential number.

Using CSVIMPORT.EXE to import inventory data

LANDesk includes a command-line utility that allows you to import inventory data into the core database. This can be useful if you're installing new devices and you have information like MAC addresses available. You can use CSVIMPORT.EXE to import this data to the core server so you can target devices ahead of time for OS deployment jobs.

CSVIMPORT.EXE requires a template file describing the field contents and what columns in the core database the data should go in. CSVIMPORT.EXE also requires the .CSV file containing the data matching the template file you specify. CSVIMPORT.EXE creates miniscan files that you can then copy to the LANDesk/ManagementSuite/LDScan directory so they get added to the core database.

Sample template file:

```
Network - NIC Address = %1%
Network - TCP/IP - Adapter 0 - Subnet Mask = 255.255.255.0
BIOS - Serial Number = %2%
BIOS - Asset Tag = %3%
Display Name = %4%
```

Note that you can include custom data in the files. The entries %1, %2, and so on refer to the first, second, and so on columns. The subnet mask in this case will be applied to all entries as 255.255.255.0. The template file can't have any header text other than the actual template information.

Sample .CSV file:

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1
0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2
0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3
0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4
0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5
0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Run CSVIMPORT with these three parameters: <templateFilename> <csvFileName> <outputDirectoryForScanFiles>. If you want the output to be entered in the core database immediately, specify your LANDesk/ManagementSuite/LDScan directory for output.

Creating custom computer names

The **Assign naming convention for target computers** page of the OS Deployment/Migration Tasks wizard lets you create computer names based on MAC addresses, text you enter, and counters (nnn...). You can also create names based on inventory data for asset tags, serial numbers, and login names by creating a COMPUTERNAME.INI file.

COMPUTERNAME.INI syntax:

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

The values returned by the .INI file substitute for the \$MAC token in the wizard's naming convention page.

You can only use the above three inventory values in the file. OS deployment checks the options in the numeric tok<x> order. All three of the above tokens don't have to be in the file. The first tok<x> option found that has an equivalent database entry substitutes for the \$MAC token for the device being imaged. For example, in the case above, if there were no asset tag or serial number entries in the database, but there was a login name, the login name would be used for the \$MAC token. If none of the options match, the MAC address is used for the \$MAC token.

The login name option returns the login name returned by the most recent inventory scan.

Using the nnn computer name token

The **Assign naming convention for target computers** page of the OS Deployment/Migration Tasks wizard includes an nnn option that substitutes for a 3-15 digit number, depending on how many n characters you specify. For each computer name template you use in the wizard, OS deployment keeps a running counter of the numbers used. This way, subsequent jobs continue where the last job left off.

Every unique template has its own counter. If you always use the same template, the counter will span jobs. If you change your template after deploying some devices and later decide to go back to the template you originally used, the counter remembers where you left off for that template and continues counting.

Customizing the SYSPREP.INF [RunOnce] section with tokenized inventory values

The SYSPREP.INF contains a [RunOnce] section that specifies programs to run after the device boots for the first time. If you add your own programs to that section, you can include database tokens on the program command line if they're useful to the program you're running. OS deployment substitutes the token you specify with corresponding information from the core database.

Sample tokens:

```
%Computer - Device Name%
%Computer - Login Name%
%Computer - Manufacturer%
%Computer - Model%
%Computer - Type%
%Computer - BIOS - Asset Tag%
%Computer - BIOS - Service Tag%
%Network - TCPIP - Address%
%System - Manufacturer%
%System - Model%
%System - Serial Number%
%Processor - Processor Count%
%Computer - Workgroup%
%Computer - Domain Name%
```

You can chain multiple tokens together. For example, to separate two tokens by a colon:

%Computer - Workgroup%:%Computer - Device Name% could return
MyWorkgroup:MyComputer.

Note: You should only use tokens that return a single value.

Using images in mixed uniprocessor and multiprocessor environments

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP images. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

Note: The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's UNATTEND.TXT file for more details. Generally, you need to remember the following when sharing uniprocessor and multiprocessor images: **Both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.**

To configure multiple processor information

1. In the Sysprep file information page of the OS Deployment/Migration Tasks wizard, select **Configure advanced multiprocessor options** and then click **Next**.
2. In the Configure multiprocessor information page, select whether you're deploying a **Windows 2000** or a **Windows XP** image.
3. Select whether the image you're using was created on a **Uniprocessor** or **Multiprocessor** device.
4. Your source and target devices have the same HAL. If your image was created on an APIC ACPI device, select **APIC**. If your image was created on a non-ACPI APIC device, select **MPS**.

Adding network adapter drivers

There are three network adapter driver detection phases that occur during on OS deployment job, as follows:

Phase 1 occurs in Windows:

NICINFO.EXE detects PnP drivers in Windows 2000/XP. It also detects Windows 9x if IE 4.02 or higher is installed. NICINFO.EXE writes the detected vendor and device ID to DOSNIC.INI on the virtual boot image.

Phase 2 occurs in DOS:

AUTODETE.EXE looks for the DOSNIC.INI left by NICINFO.EXE and reads the vendor and device ID. AUTODETE.EXE then refers to NIC.TXT to find the corresponding driver to load. It copies the driver from c:\Net\Drivers on the virtual boot image to the current RAM drive image (r:\Net by default). AUTODETE.EXE then sets the Microsoft DOS network stack configuration files, SYSTEM.INI and PROTOCOL.INI.

If DOSNIC.INI is empty, AUTODETE.EXE scans all PCI device slots looking for network adapter vendor and device IDs. If the ID found matches an entry in NIC.TXT, AUTODETE.EXE loads that driver.

Phase 3 continues in DOS:

If DOSNIC.INI is empty and AUTODETE.EXE can't match the discovered ID with NIC.TXT, it loads the driver specified in the OS Deployment/Migration Tasks wizard. If this driver doesn't load, the device will be stuck in DOS, and you'll need to reboot it manually. If no driver was specified in the wizard, AUTODETE.EXE saves an AUTODETE.LOG file to the drive root and the device boots back into the original operating system.

NICINFO.EXE and AUTODETE.EXE don't support 16-bit PCMCIA network adapters. You can load the drivers for these network adapters by selecting the appropriate driver in the OS Deployment/Migration Tasks wizard as described in Phase 3. NICINFO.EXE can detect network adapters that support CardBus.

NICINFO.EXE requires PnP support. Windows NT 4 has no PnP support.

Adding network adapter drivers

To add network adapter drivers

1. Edit the **ALTDIVERS.INI** file.
2. Edit the **NIC.TXT** file in the `..\ManagementSuite\OSD\Utilities` directory.
3. Use **COPYFILE.EXE** to insert the .DOS or .EXE driver file into the virtual boot image in `..\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG`
4. Use **COPYFILE.EXE** to insert **NIC.TXT** to the virtual boot image.

Editing the ALTDIVERS.INI file

ALTDIVERS.INI is the driver description file.

Sample entry:

```
[Intel PRO/1000 Adapters]
DRIVER=E1000.DOS
PROTOCOL=E1000
```

The description between [] can be anything. This is the text that appears in the OS Deployment/Migration Tasks wizard when you manually select a network adapter driver:

- DRIVER is the .DOS or .EXE network adapter driver.
- PROTOCOL often is the same as the driver name or the manufacturer name.

Editing the NIC.TXT file

NIC.TXT has information for detecting network adapters. You'll need to edit the NIC.TXT to add custom adapter information. Here's a sample entry:

```
ven=115D "Xircom"
dev=0003 "Xircom CardBus Ethernet 10/100 Adapter"
drv="CBENDIS.EXE"
prot="XIRCOM"
```

These are the four possible keys and values:

- **ven** is four characters (for example, 1 must be 0001); description can be anything.

- **dev** is four characters; description can be anything.
- **drv** is the driver name; default extension is .DOS.
- **prot** is the protocol, often the same as the driver name or the manufacturer.

As you can tell by looking at NIC.TXT, not all drivers have all keys.

Injecting driver changes back into the virtual boot image

To inject driver changes back into the virtual boot image, use copyfile. The syntax is:

`COPYFILE <imgfile> <srcfile> <destfile>`

Example:

```
COPYFILE c:\Program Files\LANDesk\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG  
c:\Drivers\MYNIC.DOS\Net\Drivers\MYNIC.DOS
```

Note: The <destfile> variable can't contain the drive letter designation.

You need to copy the .DOS or .EXE network adapter driver to c:\Net\Drivers and the updated NIC.TXT to c:\Net

Using the LANDesk imaging tool for DOS

Note: When you install the OS deployment and profile migration component, files for the LANDesk imaging tool are automatically installed on your core server. If you want to run the LANDesk imaging tool from a different location, you need to copy the following four files: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT, and BACKALL.BAT.

LANDesk's imaging tool for DOS (IMAGE.EXE) is a DOS-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most ATAPI CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

Limitations

IMAGE.EXE relies on the BIOS for processing disk functions. If a computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGE.EXE will also be limited.

System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- 16 MB RAM
- XMS

Getting started

IMAGE.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

Environment variables

You can use several different environment variables with IMAGE.EXE:

- **IMSG** displays a message on the screen. To create a message with IMSG, use the set command (i.e., set imsg=<include message of 80 characters or less here>).
- **IBXT** changes the method used to burn a set of CDs so that IMAGE.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1. (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGE.EXE to auto-respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.
- **IOBS=A** tests the network speed and uses the best buffer size for uploading/downloading an image.

Command-line options

You can use command-line options with IMAGE.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option to view a list of additional command-line options not explained here.

To create a compressed image to a file

Format 1: image /Ch# d:\filename.img (no validation)

Format 2: image /Ch#V d:\filename.img (validation)

Format 3: image /Ch#VB d:\filename.img (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPvV where P is the extended partition and vV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGE.EXE without any command-line options and select Create Image. The screen that lists the partitions and volumes will display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

To create an uncompressed image to a file

Format 1: image /Ch# /U d:\filename.img (no validation)

Format 2: image /Ch#V /U d:\filename.img (validation)

Format 3: image /Ch#VB /U d:\filename.img (byte-for-byte validation)

Explanation: Same as above.

To create a compressed image to a CD drive

Format 1: image /Ch# /CDx (ATAPI)

Format 2: image /Ch# /CDSx (ASPI)

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

To create an uncompressed image to a CD drive

Format 1: image /Ch# /U /CDx (ATAPI)

Format 2: image /Ch# /U /CDSx (ASPI)

Explanation: Same as above.

To restore an image from a file

Format 1: image /R d:\filename.img (no validation)

Format 2: image /RV d:\filename.img (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

To restore an image from a CD

Format 1: image /R /CDx (ATAPI)

Format 2: image /R /CDSx (ASPI)

Explanation: The x after /CD is the CD drive number to use. Omit the x (/CD or /CDS) to get a list of the devices.

To limit the file size on creation

Format: d:\filename;s

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

Issues to be aware of

- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- When restoring an image, you shouldn't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system will reboot. This is required because the partitions and file system being used by the OS have changed. If a reboot didn't occur, the OS would still think the partition and file system was as it was before the restore. This could cause data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition goes to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, then a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGE.EXE via AUTOEXEC.BAT if desired.

Using the LANDesk imaging tool for Windows

LANDesk's imaging tool for Windows (IMAGEW.EXE) is a Windows 32-based backup and restore utility that creates a snapshot of an entire partition or volume and saves it to a set of files, or saves it directly to most types of DVD+RW or CD-R/RW drives. If something should ever happen to that partition or volume, you can simply restore the snapshot image.

IMAGEW.EXE is compatible with LANDesk's imaging tool for DOS (IMAGE.EXE).

Limitations

For use with Windows 9x/Me, IMAGEW.EXE requires that the system support Int 13h extensions. If your computer BIOS limits access to the hard drive for any reason and no drive manager is available to correct the limitation, IMAGEW.EXE will also be limited on those OSes.

System requirements

- IBM-compatible personal computer with an i80386-compatible microprocessor or greater
- Windows 32-based environment with 32 MB RAM minimum recommended
- Administrator privileges when running on Windows NT, Windows 2000, or Windows XP

IMAGEW.EXE is installed as part of LANDesk OS Deployment in the \Program Files\LANDesk\ManagementSuite\osd\imaging directory.

Creating images

You can use various environment variables and command-line options to ensure that the images you create meet your requirements.

Environment variables

Environment variables for IMAGEW.EXE must be used with command-line options. The following environment variables are available:

- **IBXT** changes the method used to burn a set of CDs so that IMAGEW.EXE doesn't prompt for the last CD during a restore. Set IBXT to a value of 1 (i.e., set ibxt=1). This setting may not work with all CD-R/RW drives.
- **IAR** enables IMAGEW.EXE to auto respond to prompts and error messages when creating an image to a file. Set IAR to Y or N (i.e., set iar=Y). With this setting, all 'Y'es or 'N'o prompts that require users to press Enter are automatically responded to. You can use DOS errorlevels in a batch file to determine if the operation succeeded or failed.

Command-line options

You can use command-line options with IMAGEW.EXE. Separate the options by spaces and enter them in the order shown below. Use the /? command-line option for additional command-line options not explained here.

To create a compressed image to a file

Format 1: `imagew /Ch# d:\filename.img` (no validation)

Format 2: `imagew /Ch#V d:\filename.img` (validation)

Format 3: `imagew /Ch#VB d:\filename.img` (byte-for-byte validation)

Explanation: Replace the h with the source hard drive number from 0 to 7 and the # with the partition entry ID. For most users, the partition ID is a number from 1-4, or for volumes, a number formatted as 0xPVV where P is the extended partition and VV is the volume number in hexadecimal from 01 to FF.

If you don't know the partition or volume ID, run IMAGEW.EXE without command-line options and select Create Image. The screen that lists the partitions and volumes will also display the ID in parentheses as a hexadecimal number. You should prefix that number with a 0x on the command line.

To create an uncompressed image to a file

Format 1: `imagew /Ch# /U d:\filename.img` (no validation)

Format 2: `imagew /Ch#V /U d:\filename.img` (validation)

Format 3: `imagew /Ch#VB /U d:\filename.img` (byte-for-byte validation)

Explanation: Same as above.

To create a compressed image to a CD drive

Format 1: `imagew /Ch# /CDx`

Explanation: The h and # information is the same as above. The x after /CD is the CD drive number to use. Omit the x (/CD) to get a list of the devices.

To create an uncompressed image to a CD drive

Format 1: `imagew /Ch# /U /CDx`

Explanation: Same as above.

To restore an image from a file

Format 1: `imagew /R d:\filename.img` (no validation)

Format 2: `imagew /RV d:\filename.img` (validation if needed)

Explanation: Restores the image to the same hard drive and drive location that it was backed up from.

To restore an image from a CD

Format 1: `imagew /R /CDx`

Explanation: The x after /CD is the CD drive number to use. Omit the x to get a list of the devices.

To limit the file size on creation

Format: `d:\filename;s`

Explanation: Replace the s after the ";" with 0 for 2 GB, 1 for 698 MB, or 2 for 648 MB.

Issues to be aware of

- When running under Windows NT/2000/XP Pro, you must have administrator privileges. Under Windows 2000/XP, you can run as any user by right-clicking and selecting the Run As option.
- When creating an image, you shouldn't use the partition being backed up as the location of the image file. If you do, the partition will be updated at the same time you're trying to back it up. When you restore the partition, the file system won't be in a consistent state.
- If you create a backup without a lock being obtained, that backup may not be in a consistent state if updates to the drive were occurring during the backup.
- When restoring an image, you can't restore over the partition that contains the source image file. If you do, the restore will overwrite the file system structures and the image file itself.
- After restoring, the system may need to reboot. This is required under certain conditions and determined by the program. If you don't reboot when asked, the OS will think the partition and file system is as it was before the restore, potentially causing data corruption. You can override a command-line restore with /RN, but it should only be used by advanced users who know it's safe to not reboot.
- When you do a command-line restore, the restored partition will go to the same hard drive number and physical location on the drive as where it was backed up from. If it was a volume and there is no extended partition now at that location, then it will attempt to create the original extended partition. If it can't create the extended partition, it will be restored as a primary partition. If it was a primary partition and now an extended partition encompasses that location, then it will be restored as a volume. If an existing partition or volume occupies the same starting location as the partition to be restored, a warning message is issued before overwriting that partition or volume.
- To restore via booting the CD, you must have an ATAPI CD drive. For SCSI drives, you must create your own CDBOOT.F35 file to load the appropriate DOS ASPI drivers and launch IMAGEW.EXE via AUTOEXEC.BAT if desired.

Appendix C: Additional software distribution information

This chapter explains how to use LANDesk Management Suite's software distribution (SWD) to distribute software and files to devices throughout your network.

Read this chapter to learn about:

- Scripting guide for .CFG files
- Troubleshooting .CFG files and their packages
- Scripting guide for deployment scripts (.INI files)
- Understanding Software Distribution error codes
- Files used in Software Distribution

Scripting guide for .CFG files

This section describes what you can do with scripts and scripting commands as you build a software distribution package. At the end of this section, there's a sample script with remarks that explain the important parts of the script.

For detailed instructions about creating and modifying .CFG files, see the Package Builder online help. Click **Start | Programs | LANDesk Management | LANDesk Enhanced Package Builder**. Click **Help | Index** and select the following online help topics:

- Getting started with Package Builder
- Creating a simple installation
- Package Builder commands
- How does Package Builder do an installation?
- Using variables in commands and assigning values

Scripting basics

The Package Builder wizard steps you through the process of creating a software distribution package. The wizard saves the commands required to perform the same installation on other devices. It writes these commands to an ASCII file with a .CFG extension. You can edit this script file after creating it in Package Builder, or you can create one from scratch and build it into a package.

The Package Builder online help provides syntax information for each of the script commands. To access the help for a specific command, highlight a command in the left panel and press the **F1** key.

To access a specific script file, start Package Builder and click **File | Open**. Browse to the Configs folder in the Package Builder working folder and select a file.

Once a script has been modified, click **Build | Build** to build the script into a package.

Script commands

Each script includes two sections. Specific commands at the top of the script define the operating parameters, and the balance of the commands describes the installation of the application included in the software distribution package.

All of the commands included in a script can be grouped into one of these functional categories:

- Base Installation
- Appearance
- Messages & Input
- System Changes
- If Conditions
- Defaults & Calls

These categories contain related commands that describe the installation process for each package. Some commands describe the operating parameters of the installation and must be placed at the top of the script file. For details about each command, see the Package Builder online help.

Editing packages with the Package Builder

The Package Builder interface is divided into three areas:

- In the left pane, the functional categories are listed. Expand each functional category to display the individual commands within that category.
- The right pane is divided into two screens: The upper portion displays the script itself. The lower portion is a GUI template that contains entry boxes for the parameters of the highlighted command.

To see the details of a command in the script, highlight the command and view the parameter details in the lower portion of the screen.

To add a new command to the script, select the location in the script where the command should be located. Next, highlight the command in the left pane. Now complete the syntax template in the lower portion of the screen. When you've selected the command parameters, click **Add** to insert the new command.

Simple sample script

This script contains some of the commands used to install Package Builder on a package-building computer. Major sections or commands are described with remarks (REM).

```
REM This is the Package Builder installation
REM Set screen graphics environment
SCREENCOLOR: (0,0,255), (0,0,255)
ANIMATION: "W:\Software\Install\Intel\duck\DISK01.BMP",
"W:\Software\Install\Intel\duck\DISK02.BMP",
"W:\Software\Install\Intel\duck\DISK03.BMP",
"W:\Software\Install\Intel\duck\DISK04.BMP",
"W:\Software\Install\Intel\duck\DISK05.BMP",
"W:\Software\Install\Intel\duck\DISK06.BMP",
"W:\Software\Install\Intel\duck\DISK07.BMP",
"W:\Software\Install\Intel\duck\DISK08.BMP",
"W:\Software\Install\Intel\duck\DISK09.BMP",
"W:\Software\Install\Intel\duck\DISK10.BMP",
"W:\Software\Install\Intel\duck\DISK11.BMP",
"W:\Software\Install\Intel\duck\DISK12.BMP",
"W:\Software\Install\Intel\duck\DISK13.BMP"
SCREENGRAPHIC: "W:\software\INSTALL\Intel\OAKLAN~1.BMP", topleft
REM TITLE: "LANdesk Management Suite", fontsize=25, color=yellow
REM SUBTITLE: "Package Builder", fontsize=18, italic, color=yellow
REM Configure uninstallation options
UNINSTALL: yes, removegroup, packagename="Package Builder"
UninstallBeginPrompt: "Do you wish to remove the LANdesk Management
Suite Package Builder programs and directories from your system?"
UninstallEndPrompt: "LANdesk Management Suite Package Builder programs
and directories have been successfully removed from your system."
REM Check for sufficient disk space before installation
IF DISKSPACE() < 4000K
BEGINFIRSTSCREEN caption="Not Enough Disk Space", Package Builder
requires 4 MB of disk space. Please arrange your hard disk so that a
sufficient amount of disk space is available.
ENDFIRSTSCREEN
REM This is only shown if there is less than 4 MB of disk space.
```

```
ENDIF
REM Define splash screen text
BEGINFIRSTSCREEN caption="LANDesk Management Suite Package Builder",
This installation program will set up LANDesk Management Package
Builder onto your hard disk. Contact your LANDesk Software Customer
Support representative if there are problems setting it up on your
computer.
ENDFIRSTSCREEN
REM Define default directory from which to work. Notice the variable
$ProgFilesDir$ comes from a Windows system environment variable. The
DEFAULTDIR command must be used before any file commands are used.
DEFAULTDIR: "$ProgFilesDir$\Intel\Package Builder", prompt="Please
enter the drive and directory:", caption="Directory Name", text="The
software will install onto your system in a directory. Please accept
the suggested directory location or type in one of your own. Make
certain to provide both a drive letter and the directory name."
REM Add files common to all versions of Package Builder. Only one has
been included in this sample script.
FILE: "CTL3D.000", overwrite=yes,
From="W:\Software\Install\Intel\CTL3D.DLL"
REM Install registry information
BEGINREGISTRY
KEY: new, "HKEY_CLASSES_ROOT\CFG"
VALUE: reg_sz, replace, "Default", "txtfile"
ENDREGISTRY
REM Setup Windows menu items
WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\Builder.exe",
"Package Builder", replace, allusers
WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\Replicator.exe",
"Package Builder wizard", replace, allusers
WINITEM: "LANDesk Management Suite", "$DEFAULTDIR$\ENUBLDRI.hlp",
"Package Builder wizard help", replace, allusers
REM Define and display final screen
BEGINLASTSCREEN caption="LANDesk Management Suite Package Builder",
The installation of the Management Suite Package Builder is now
complete.
ENDLASTSCREEN
```

Registry commands

Commands that modify the registry begin and end with BeginRegistry and EndRegistry commands. In between these commands are the commands that identify the registry key and the value. The Package Builder wizard flags two keys as dangerous:

- \HARDWARE
- \SYSTEM\CURRENTCONTROLSET

These keys are considered dangerous because they are usually not compatible with any device other than the package-building computer. When these keys are modified, the Package Builder wizard places such commands within an IF \$DANGEROUS\$ = "TRUE" statement. If the changes to these keys are compatible with your target devices and you want them executed, you must define a \$DANGEROUS\$ variable at the top of the script and set its value to TRUE.

Launching a package from a package

You can specify INST32.EXE on the command line of a RunAtExit command in one package in order to launch another package. The syntax is:

```
RunAtExit "INST32.EXE PACKAGENAME.EXE"
```

If the package is found on the network, this is more efficient than just running "PACKAGENAME.EXE." It allows you to specify a package name via an HTTP path. For example:

```
http://myservername/packages/PACKAGENAME.EXE
```

Sample script with more complex commands

This next script is organized into sections with a brief explanation for each. Any applications launched by a RunAtStart or RunAtMiddle command must be closed for the script to continue processing.

The beginning section of this script enables you to include a window title, package name, animated or still graphics, and audio, as well as color and font selections. A RunAtStart command enables you to execute an external application at the beginning of the installation.

Next, the BeginFirstScreen command enables you to inform the user about the installation by displaying a text message. Finally, the Backup command indicates that any files that are to be replaced will be backed up, and the OverWriteFile command indicates that the user will be prompted before any existing files are overwritten.

```
ANIMATION: "C:\WINDOWS\CIRCLES.BMP", "C:\WINDOWS\CARVED~1.BMP",
"C:\WINDOWS\BUBBLES.BMP", "C:\WINDOWS\BLUERI~1.BMP",
"C:\WINDOWS\BLACKT~1.BMP"
RUNATSTART: "c:\program files\accessories\mspaint.exe"
TITLE: "Package Builder Functionality Script for Windows 98", bold
INTROSCREEN: "C:\WINDOWS\SETUP.bmp", waittime=5, full
INTROSOUND: "C:\WINDOWS\MEDIA\START.WAV"
SCREENCOLOR: magenta, yellow
SCREENGRAPHIC: "C:\WINDOWS\PINSTR~1.BMP", topleft
FONTNAME: "Tahoma"
BEGINFIRSTSCREEN title="First Screen", caption="Screen #1"
This is the text that appears on the first screen.
ENDFIRSTSCREEN
BACKUP: YES
OVERWRITEFILE: ask
```

The following examples show different prompt options. Text for each prompt can be modified.

```
CancelPrompt: "Cancel?"
CopyFilePrompt: "UPLOAD IN PROGRESS"
OkPrompt: "GOOD JOB"
QuitPrompt: "Do you really want to quit?"
CopyTitlePrompt: "Copying..."
NextPrompt: "Next"
BackPrompt: "Back"
NoPrompt: "No"
YesPrompt: "Yes"
```

This section runs an external application and waits for that application to be closed before continuing. When the script continues, the user is prompted for input. Based on the selected option, the application continues and copies a file on the local drive or exits.

USER'S GUIDE

```
RUNATMIDDLE: "c:\windows\calc.exe"
ASK1: Yesno, caption="Sample question.", text="This is an example using
Yes / No buttons. Choose `Yes' to continue, `No' to exit."
IF $ASK1$= "yes"
WINGROUP: "New Program Group", prompt="Select a group",
caption="Program Group selection", text="Please select a program
group."
ELSE
IF $ASK1$= "No"
EXITMESSAGE
Sorry you had to leave so soon!
EXIT
ELSE
ENDIF
ENDIF
PROGRESSBAR: 302K
COPY: "C:\windows\setup.bmp", "C:\windows\temp\p1.bmp"
RENAME: "C:\windows\temp\p1.bmp", "C:\windows\temp\renamed p1.bmp"
```

This section launches an application as the last command before the script is completed. The **RunAtExit** command does not have to be the last line of the script.

This section also places a shortcut on the desktop and creates an uninstall package.

```
RUNATEXIT: "C:\WINDOWS\CDPLAYER.EXE"
BEGINLASTSCREEN title="Last screen", caption="The last screen"
This should be the last screen you see.
ENDLASTSCREEN
SHORTCUT: "c:\windows\notepad.exe", "NOTEPAD",
dir="c:\windows\desktop\"
UNINSTALL: yes, makeicon, removegroup, packagename="Package Builder
Functionality"
```

Processing custom scripts

Custom scripts that control scheduled tasks (**Tools | Distribution | Scheduled tasks**) are processed in three sections:

- **Premachine:** The Premachine section of the custom script is processed first, and only once at the start of the task. Use this section for tasks that have no targeted device, and/or for Targeted Multicast. During the Premachine section of the script, only local commands, LOCxxx, should be used.
- **Machine:** The commands in this section of the script run second and only once per targeted device. These commands can use either the remote or local execution commands, and are primarily used for remotely executing SDCLIENT.EXE. Before the commands in this section of the script can be performed, the SWD agent must be installed on the targeted devices.
- **Postmachine:** This section is processed last, and again, only once after all devices have been processed. Software distribution does not add commands to this section, and it only supports the local commands, LOCxxx. The commands in this section won't be processed if devices in the task can't run them. The InventoryScanner.ini script that comes with Management Suite contains details about the script commands.

Custom Script Commands

Custom scripts support various local and remote commands:

- **LOCEXEC:** Local execute, this command is used to execute an application on the local device, which is always the core server.
- **LOCDEL:** Local deletion, deletes a file on the local device.
- **LOCMKDIR:** Local make folder, creates a folder on the local device.
- **LOCRD:** Local remove folder, this command is used to remove a folder on the local device.
- **REMCOPY:** Remote copy, copies a file from the local device to a remote device.
- **REMEXEC:** Remote execution, executes an application on the specified remote device.
- **REMDEL:** Remote deletion, deletes a file on the remote device.
- **REMMKDIR:** Remote make folder, this command creates a folder on the remote device.
- **REMRD:** Remote remove folder, this command deletes a folder on the remote device.

Command-line parameters

Software distribution is facilitated by a deployment script. SDCLIENT.EXE manages the packages using command-line parameters from the script file that are passed to the application.

SDCLIENT.EXE supports the following command-line parameters:

```
sdclient.exe /p="<package path>" [/g=<pkg guid>] [/All] [/R] [/N] [/An]
[/Ac] [/Ab] [/fui] [/msi] [/exe] [/bw=xxx] [/E]
```

Parameter name	Description
/p=<package path>	Package Path. The package path must be specified, regardless of the package type. This parameter specifies the UNC or URL path to the package

that is to be installed on the local device.

/g=<pkg guid>	Package GUID. For SWD or AutoInstall packages. This parameter specifies the GUID for the package. The package GUID is used to check the local .CFG file cache for a copy of the package's .CFG file.
/All	Uninstall Flag. This flag is set to indicate that the SWD or MSI package should be uninstalled rather than installed. This flag is case-sensitive (/all won't work).
/R	Always Reboot Flag. This flag indicates that the device should always be rebooted after the package installation. Not all MSI packages follow this guideline.
/N	Never Reboot Flag. This flag indicates that the device should never be rebooted after the package installation.
/An	Silent Installation Flag. This flag indicates that the installation should be silent. This means that no UI, or the smallest amount of UI possible, should be displayed during the installation.
/Ac	Disable Cancel Flag. This flag prohibits the user's ability to cancel the installation.
/Ab	No Background Flag. This flag only applies to SWD packages. When a package is being installed, the blue background won't be displayed.
/fui	Full UI Flag. This flag indicates that the full UI for legacy and MSI packages should be used.
/msi	MSI Package Flag. This flag indicates that the package path points to an MSI package file.
/exe	Executable Package Flag. This flag indicates that the package path points to a legacy package or a generic executable file.
/bw=xxx	Bandwidth Requirements. Specifies a minimum bandwidth requirement for the package script to be run.
/F	Generic File Flag. This flag causes SDCLIENT.EXE to download the file to the LDCLIENT folder.
/msg=""	Sends a message to the core server while the task is executing. This message appears in the task status inside the Scheduled tasks window's Message column.

HTTP and UNC paths

These are examples of software distribution .INI files that reflect the differences between HTTP and UNC path script files.

HTTP path script file:

```
; This file was generated by Desktop Manager
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=http://<web
server>/packages/test package.exe -g={6DD454C0-11D3A0D1-a000B3B5-
9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

UNC path script file:


```
; This file was generated by Desktop Manager  
[MACHINES]  
REMEEXEC0=C:\Program Files\LANDesk\LDCClient\sdclient.exe -  
p=\\sample_core\onefile\test package.exe -g={6DD454C0-11D3A0D1-  
a000B3B5-9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

Notice that both .INI files have similar elements. In the MACHINES section, the -P option designates the path where the device will download the software package. In the HTTP example, the path is `http://<web server>/packages/test package.exe`.

The next option is the -G option, which is the GUID, a unique number identifier for each package. This number identifier is generated by the Package Builder, and it helps prevent confusion during installation between packages with similar names.

Troubleshooting .CFG files and their packages

Deciding what works and what doesn't work is the first step in script debugging. These are some basic troubleshooting tips that can help you resolve script errors:

- Create a new script that consists of only the portion of the script that produces an error. Check the functionality of this script and modify as required using the online command help.
- Compare the new script to an existing script to check for syntax.

Use the following guidelines when you create packages on your package-building computer. These tips will help you avoid unnecessary errors.

Using commands

Don't pass variables to the DLL Load command in Package Builder

If you create a package that depends on passing a variable into the DLL Load command, it won't work if the variable doesn't arrive at the correct time. If the .DLL doesn't receive the expected variable, the package won't complete the installation correctly. To avoid this problem, don't pass variables into the DLL Load command; the other DLL parameters work correctly.

Using the Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands

The Package Builder RunAtMiddle, RunAtStart, and RunAtExit commands require the full path to the executable to run correctly. Also, the RunAtMiddle command must be positioned in the script after the DEFAULTDIR function to work correctly. RunAtStart and RunAtExit commands can be anywhere in the script and will run correctly.

Rebooting during package creation

When using the Package Builder wizard to create a package, you may be prompted to reboot the package-building computer. In many cases, rebooting before completing the package-building process causes the package to improperly install at the device. The application becomes configured for the package-building computer rather than the targeted device. However, in some cases, the reboot is required because the installation program accesses the installation CD after reboot.

You need to test the resulting package to determine whether you can stop the installation process and create the package before the reboot, or whether you need to reboot the package-building computer during the software installation and then continue to create the package.

Creating and naming software distribution packages

Package names can't be changed once they're created

You can't change a package name once you complete the package creation step. If you attempt to directly change the filename, your users can't access that package correctly.

Package names can't include hyphens or periods

If you use hyphens or periods in a package name, the package-creation process will truncate the name when it encounters them. You can still access the package in a script, and users can install it, but the truncated name might be confusing. Don't use hyphens or periods in a package name. You can use the underscore (_) character instead.

We recommend that you create a new working folder each time you begin creating a package. To create this folder, start the Package Builder wizard, and click Scan Options. In the Temporary Work Directory box, either type in the full path to a folder or browse to its location. Package Builder prompts you for permission to create a folder that does not already exist.

Store only software distribution packages in your distribution location

You should only keep packages in the Web server location or UNC folder that you set up for software distribution. If you store other types of executable files in this folder, they may be confused with packages when you're creating distribution package scripts. If you create a distribution script for an executable that's not a package, the distribution will fail. Store only software distribution packages in your distribution location.

For more information about creating and modifying packages, see the topic "Working with the Package Builder" in the Package Builder online help.

File collections can't contain more than 296 files

When you create a file collection package, you can add as many as 296 separate files or folders. If you attempt to add more than 296 items, the file collection stops. Files contained in an included folder count as one item, not as separate files.

Scripting guide for deployment scripts (.INI files)

You don't have to use the Create Software Distribution Script window to create the deployment script file. A deployment file is an .INI file containing the settings the device should use for installing a package. You can create your own deployment files in a text editor such as Notepad if you prefer.

A software distribution .INI script file has these components:

```
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_95.exe"
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-
66E3BC2DF01A0D4B2F88670DE4}
/Ac
/N
```

REMEXEC0 command parameters

The parameters for the REMEXEC0 command have been placed on separate lines to make the components more visible. When placed in an .INI file, the command needs to be on one line.

REMEXEC0 is the Remote Execute command. If you want to use more than one REMEXEC0 command in a single script file, increment the command each time it is used. For example, if you used three REMEXEC calls in a single .INI file, they should be REMEXEC0, REMEXEC1, and REMEXEC2. These commands don't need to increment if they're in separate files.

The C:\Program Files\LANDesk\LDClient parameter is the correct path to the SWD agent.

The /p parameter is the path statement where the device can download the package. For example:

/p="http://computer_name/95Packages/Acro32_95.exe"

The /g parameter points to a GUID identification number for the package. For example:

```
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-
66E3BC2DF01A0D4B2F88670DE4}
```

If you use this parameter, the device will only download the package with that exact ID number. Use the Create Distribution Script window to generate this ID number, because it's embedded in the software package.

The /Ac parameter hides the install from users. They can only cancel the installation if they're prompted for something. The /Ab parameter hides the background. The /An parameter hides all of the UI and prevents any interaction (prompts) from reaching the users.

The /Ah+ parameter heals a package that was previously installed, without prompting the user. The /Ah- parameter reinstalls a package that was previously installed, without prompting the user.

The /N parameter doesn't force a reboot on the device after the package is installed. The /R parameter forces a reboot on the device after the package is installed. If you don't use either the /N or /R parameters, the device will reboot only if files in use were updated or a reboot is needed to complete the installation.

An optional /D parameter opens a debug window used to view operational parameters for SDCLIENT.EXE. The debug window displays the package path and name, the GUID, any error or message codes, as well as the exit code returned to the Scheduled Tasks window.

If the software distribution script is designed to uninstall an existing application, two uninstall option parameters can be used:

- The /Au parameter uninstalls the last instance of a package and rolls back one install instance.
- The /All parameter uninstalls all instances of a package and completely removes the package.

If you follow these guidelines, you can create your own software distribution scripts and schedule them to be sent to devices. These scripts are stored in the DTM\Scripts folder on the core server.

Understanding software distribution error codes

From the console, the right panel in the **Scheduled tasks** window displays the task status. If you click Failed under the task, you can see devices that failed the job and the resulting messages and logs. The status and errors are logged to the following files:

- If the error occurred while attempting to access the package, the error is logged in the AICLIENT.LOG file.
- If the error occurred while processing the package (for example, copying files), the error is logged in the INST32.LOG file.
- The SDCLIENT.LOG file contains general summary information about each installation request received from the core server.

These log files are stored on each device. The following table lists the error codes you may encounter in these files.

Error code	Definition
101	The user cancelled the install.
102	File access was denied.
103	The password used isn't valid.
104	No network found, or incorrect path provided.
105	A download error occurred.
106	A socket could not be created.
107	Unable to open an HTTP session.
108	A CFG download error occurred.
109	A save CFG error occurred.
110	No save CFG folder exists.
111	A file access error occurred.
112	A get CFG error occurred.
113	Unable to create a backup CFG.
114	A spawn error occurred because another package is already being installed.
117	The backup directory can't be created.
180	Networking error. Can't initialize.
188	Timed out while downloading over HTTP.
189	HTTP connection aborted.

191	Host not found.
197	HTTP file not found.
201	The UNC file cannot be found.
202	The file was not found on the installation disk.
203	Unable to create a file in the specified location.
204	Not enough disk space on the destination drive for installation.
205	An invalid drive was specified, or the drive required for this install was not available.
206	The file has a long filename and can't be installed by the 16-bit install program. You still have the option to continue to install other files.
207	The specified file is not an executable.
208	Multiple uninstall registry entries exist with the same source path.
209	Unable to locate the uninstall executable.
210	Encountered an invalid compressed file, or HTTP error(s).
211	A successful AFXSOCKETINIT command must occur before using this API.
212	The network subsystem failed.
213	No more file descriptors are available.
214	The socket can't be created. No buffer space was available.
215	The specified address was already in use.
216	The connection attempt was rejected.
217	The provided host address was invalid.
218	The network can't be reached from this host at this time.
219	The attempt to connect timed out without establishing a connection.
220	The virtual circuit was aborted due to a timeout or other failure.
221	The virtual circuit was reset at the remote site.
222	A non-stated HTTP error occurred.
223	An HTTP error occurred; the file wasn't open for reading.
224	An HTTP error occurred; no content-length setting provided.
225	An HTTP error occurred; not enough memory available.
226	A memory allocation error occurred.
227	Unable to read the file.
228	Insufficient memory available.
229	The .CFG file has an error at line XX.

- 240 The temporary path specified is invalid. It can't be accessed or created. The target computer has a configuration problem.
- 301 This application has never been installed on this computer; it can't be uninstalled.

Files used in script-based software distribution

This is a list of the files used in SWD, as well as descriptions of how they work together. You can use this information to customize how packages are created, stored, and deployed in your organization.

These files are installed at the core server:

- ManagementSuite\CUSTJOB.EXE
- ManagementSuite\SDMAKINI.DLL
- ManagementSuite\LANDesk.ManagementSuite.WinConsole.dll
- ManagementSuite\INSTALL\EN_PKG_BLD\SETUP.EXE
- ManagementSuite\LDLOGON\SDCLNSTL.EXE

These files are installed at the device:

- C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE
- C:\Program Files\LANDesk\LDClient\AICLIENT.DLL
- C:\Program Files\LANDesk\LDClient\SDMCACHE (this is an empty folder)
- C:\LDCLIENT.LOG (this file is created by the SDCLIENT.EXE file)
- INST32.EXE
- EUNINST32.DLL (or other locale-specific resource file)
- \$WINDIR\$aiclient.log
- \$WINDIR\$inst32.log

File descriptions

SETUP.EXE: This standalone, binary installation file is used to create package-building computers, placing the Package Builder, Package Builder wizard tools, and accompanying online help files onto the computer. Each application that you package with Package Builder is made into a self-extracting .EXE.

If you're using the Web Console, you must copy the .EXE to the packages folder on your Web server for users to access.

SETUP.EXE installs the following types of files on the package-building computer in the Program Files\Intel\Package Builder folder:

- BUILDER.EXE: Enhanced Package Builder executable
- ENUBLDR.DLL: Enhance Package Builder resource file
- REPLICATOR.EXE: Package Builder wizard executable
- ENUREPLC.DLL: Package Builder wizard resource file
- BASIC.CFG: A simple installation script for building a software distribution package
- TYPICAL.CFG: A more complex installation script for building a software distribution package
- ENUBLDR.HLP: Help file for the Package Builder
- ENUBLDRI.HLP: Help file for the Package Builder wizard

CUSTJOB.EXE: This file is launched directly by the Scheduler when a job is to begin.

SDC_INSTALL.INI: This job script is processed by CUSTJOB.EXE. It copies SDCINSTL.EXE to a remote device and then executes it on that device via the standard LANDesk agent (CBA). This file is placed in the DTM\Scripts folder.

SDCLNSTL.EXE: This file installs the SWD client files SDCLIENT.EXE and AICLIENT.DLL on Windows 95/98 and Windows NT/2000/2003/XP devices. This file is placed in the DTM\LDLogon folder on the core server.

SDCLIENT.EXE: This file is ultimately placed on the device in the C:\Program Files\LANDesk\LDClient folder. It's invoked with command-line parameters that include the URL or UNC path of the distribution package to be installed. This invocation is normally a result of the core server Scheduler calling CUSTJOB.EXE.

AICLIENT.DLL: This file is called by SDCLIENT.EXE; it's copied to the same folder as SDCLIENT.EXE.

INST32.EXE: This is the actual installer program. It's embedded within every self-extracting package. It's also installed into the LDClient folder and launched by SDCLIENT.EXE whenever a request to install a software package is received.

ENUINST32.DLL: This is a locale-specific resource file, and its name varies with the locale.

AICLIENT.LOG: This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to AICLIENT.LOG1. When the new AICLIENT.LOG file exceeds the 50 KB limit, AICLIENT.LOG1 is renamed to AICLIENT.LOG2. It's incremented one more time to AICLIENT.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current AICLIENT.LOG file.

INST32.LOG: This is a rolling log. Once it exceeds 50 KB, the next install causes it to be renamed to INST32.LOG1. When the new INST32.LOG file exceeds the 50 KB limit, INST32.LOG1 is renamed to INST32.LOG2. It's incremented one more time to INST32.LOG3. It is deleted the next time the 50 KB limit is exceeded on the current INST32.LOG file.

Appendix D: Additional security scanner information

LANDesk Security Suite includes the Security and Patch Manager tool as the main component of its comprehensive security management solution. Use the Security and Patch Manager tool to download updates for various security content type's definitions and patches; create, configure, and run security assessment scans and remediation scans; enable security alerts; generate security reports, and more. Security and Patch Manager basics are covered in the Using Security and Patch Manager and Security and Patch Manager help chapters.

This chapter provides supplemental information about using the security (vulnerability) scanner.

Read this chapter to learn about:

- Using command-line parameters for the vulnerability scanner

Using command-line parameters with the vulnerability scanner

The security (vulnerability) scanner is called VULSCAN.EXE and it supports the following command-line parameters:

Parameter name	Description
General parameters	
/AgentBehavior=AgentBehaviorID	Overwrites the default agent behavior of the security scanner.
/ShowUI	Shows the scanner UI on an end user device.
/AllowUserCancelScan	Shows a Cancel button on the scanner UI that lets the end user cancel the scan.
/AutoCloseTimeout=Number	Timeout value in seconds. If set to -1, then UI waits for the end user to close manually.
/Scan= String (0-8)	Number codes for different types: 0 - vulnerability 1 - spyware 2 - security threat 3 - LANDesk updates 4 - custom definition 5 - blocked application 6 - software updates 7 - driver updates 8 - antivirus 100 - all types
/Group= Int	Group id for scanning, overrides scan parameter if present

/AutoFix= true or false

String telling the scanner whether autofix is enabled or disabled.

Repair parameters

/Repair (group = or vulnerability=)

Tells the scanner which group or vulnerability to repair (remediate). Can be all.

/RemovePatch

Use a unique patch name.

/RepairPrompt

A string text message that prompts the end user.

/AllowUserCancelRepair

A string that allows the end user to cancel repair if using a repair prompt.

/AutoRepairTimeout=Number

A timeout value of repair prompt in seconds. If it's set to -1, then the UI waits for user to close manually.

/DefaultRepairTimeoutAction

A string for the default action for vulscan to take if timeout expires for repair prompt, acceptable values. Values include: start and close.

/StageOnly

A string to retrieve patch or patches needed for repair but don't install.

/Local (get files from peer)

Forces peer only download.

/PeerDownload

Same as /local.

/SadBandwidth=Number

Maximum percentage of bandwidth to use when downloading.

Reboot parameters

/RebootIfNeeded

Use this parameter to reboot a machine if needed

/RebootAction

A string that determines vulscan's reboot behavior when repairing, acceptable values: always, never, or empty (anything else), If anything else, then vulscan will reboot if needed.

/RebootMessage

A string that displays text message to user in a reboot prompt.

/AllowUserCancelReboot

A string that allows user to cancel reboot if using a reboot prompt.

/AutoRebootTimeout=Number

Timeout value of reboot prompt in seconds, if set to -1, then UI waits for user to close manually.

/DefaultRebootTimeoutAction

A string that determines the action for vulscan to take if timeout value expires for reboot prompt, acceptable values: reboot, close, snooze.

/SnoozeCount=Number

Number of snoozes, vulscan decrements each time the user clicks snooze on the reboot prompt.

/SnoozeInterval=Number

Number of seconds for vulscan to sleep between snoozes.

MSI parameters

/OriginalMSILocation=path	Path to original MSI location.
/Username	Username for MSI directory.
/Password	Password for MSI directory.
Disable parameters	
/NoElevate	Do not launch vulscan via core tech.
/NoSleep	Prevents sleeping during definition scan (1/18th).
/NoSync	Doesn't get mutex, can multiple instances.
/NoUpdate	Don't get a new version of vulscan.
/NoXML	Don't look for msxml.
/NoRepair	Same as autofix=false. Overrides autofix setting if present.
Data files parameters	
/Dump=	Dumps vulnerability data directly from Web service.
/Data	Sucks in vulnerability data (from /dump).
/O=Path\Filename	Output scan results.
/I=Path\Filename	Input scan results.
/Log=Path\Filename	Overrides log file name.
/CoreServer=Server name	Identifies core server name.
/Reset	Removes delta file base information (wipes out application data directory).
/Clear or /ClearScanStatus	Clears all vulnerability scan information.

Context-sensitive help

This chapter provides information about activating your core server with a valid LANDesk software license, and starting the console to access and utilize all of the LANDesk tools.

Read this chapter to learn about:

- Activating the core server
- Starting the console
- Changing the core server connection

Activating the core server

LANDesk uses a central licensing server to help you manage your core server's product and node licenses. To use LANDesk products, you must obtain a user name and password that will activate the core server with an authorized certificate. Activation is required on each core server before you can use LANDesk products on that server. You can activate each core server either automatically through the Internet or manually by e-mail. You may need to reactivate a core server in the event that you significantly modify its hardware configuration.

On a periodic basis, the activation component on each core server will generate data regarding:

- The precise number of nodes you're using
- The non-personal encrypted hardware configuration
- The specific LANDesk programs you're using (collectively, the "node" count data)

No other data is collected or generated by the activation. The hardware key code is generated on the core server using non-personal hardware configuration factors, such as the size of the hard drive, the processing speed of the computer, and so on. The hardware key code is sent to LANDesk in an encrypted format, and the private key for the encryption resides only on the core server. The hardware key code is then used to create a portion of the authorized certificate.

After installing a core server, use the Core Server Activation utility (**Start | All Programs | LANDesk | Core Server Activation**) to either activate it with a LANDesk account associated with the licenses you've purchased or with a 45-day evaluation license. The 45-day evaluation license is for 100 nodes. There are two types of licenses, device and server. Any time you install LANDesk agents on a server operating system, such as Windows 2000 Server or Windows 2003 Server, that installation consumes a license for a server. Rollup core servers don't need to be activated.

You can switch from a 45-day evaluation to a paid license at any time by running the Core Server Activation utility and entering your LANDesk username and password.

Each time the node count data is generated by the activation software on a core server, you need to send the node count data to LANDesk, either automatically by the Internet or manually by e-mail. If you fail to provide node count data within a 30-day grace period after the initial node count verification attempt, the core server may become inoperative until you provide LANDesk with the node count data. Once you send the node count data, LANDesk will provide you with an authorized certificate that will allow the core server to work normally once again.

Once you've activated a core server, use the product licensing dialog (**Configure | Product licensing**) to view the products and the number of authorized nodes purchased for the account the core server authenticates with. You can also see the date the core server will verify node count data with the central licensing server. The core server doesn't limit you to the number of authorized nodes you purchased.

About the Core Server Activation utility

Use the Core Server Activation utility to:

- Activate a new server for the first time
- Update an existing core server or switch from a trial-use license to a full-use license
- Activate a new server with a 45-day trial-use license

Start the utility by clicking **Start | All Programs | LANDesk | Core Server Activation**. If your core server doesn't have an Internet connection, see [Manually activating a core or verifying the node count data](#) later in this section.

Each core server must have a unique authorized certificate. Multiple core servers can't share the same authorization certificate, though they can verify node counts to the same LANDesk account.

Periodically, the core server generates node count verification information in the "%Program Files\LANDesk\Authorization Files\LANDesk.usage" file. This file gets sent periodically to the LANDesk licensing server. This file is in XML format and is digitally signed and encrypted. Any changes manually made to this file will invalidate the contents and the next usage report to the LANDesk licensing server.

The core communicates with the LANDesk licensing server via HTTP. If you use a proxy server, click the utility's **Proxy** tab and enter your proxy information. If your core has an Internet connection, communication with the license server is automatic and won't require any intervention by you.

Note that the Core Server Activation utility won't automatically launch a dial-up Internet connection, but if you launch the dial-up connection manually and run the activation utility, the utility can use the dial-up connection to report usage data.

If your core server doesn't have an Internet connection, you can verify and send the node count manually, as described later in this section.

Activating a server with a LANDesk account

Before you can activate a new server with a full-use license, you must have an account set up with LANDesk that licenses you for the LANDesk products and number of nodes you purchased. You will need the account information (contact name and password) to activate your server. If you don't have this information, contact your LANDesk sales representative.

To activate a server

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use.
4. Click **Activate**.

Activating a server with a trial-use license

The 45-day trial-use license activates your server with the LANDesk licensing server. Once the 45-day evaluation period expires, you won't be able to log in to the core server, and it will stop accepting inventory scans, but you won't lose any existing data in the software or database. During or after the 45-day trial use license, you can rerun the Core Server Activation utility and switch to a full activation that uses a LANDesk account. If the trial-use license has expired, switching to a full-use license will reactivate the core.

To activate a 45-day evaluation

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Activate this core for a 45-day evaluation**.
3. Click **Activate**.

Updating an existing account

The update option sends usage information to the LANDesk licensing server. Usage data is sent automatically if you have an Internet connection, so you normally shouldn't need to use this option to send node count verification. You can also use this option to change the LANDesk account the core server belongs to. This option can also change a core server from a trial-use license to a full-use license.

To update an existing account

1. Click **Start | All Programs | LANDesk | Core Server Activation**.
2. Click **Update this core server using your LANDesk contact name and password**.
3. Enter the **Contact name** and **Password** you want the core to use. If you enter a name and password that's different than the one used to originally activate the core, this switches the core to the new account.
4. Click **Activate**.

Manually activating a core or verifying the node count data

If the core server doesn't have an Internet connection, the Core Server Activation utility won't be able to send node count data. You'll then see a message prompting you to send activation and node count verification data manually through e-mail. E-mail activation is a simple and quick process. When you see the manual activation message on the core, or if you use the Core Server Activation utility and see the manual activation message, follow these steps.

To manually activate a core or verify the node count data

1. When the core prompts you to manually verify the node count data, it creates a data file called {languagecode}-activate.{datestring}.txt in the "\Program Files\LANDesk\Authorization Files" folder. Attach this file to an e-mail message and send it to licensing@landesk.com. The message subject and body don't matter.
2. LANDesk will process the message attachment and reply to the mail address you sent the message from. The LANDesk message provides instructions and a new attached authorization file.
3. Save the attached authorization file to the "\Program Files\LANDesk\Authorization Files" folder. The core server immediately processes the file and updates its activation status.

If the manual activation fails or the core can't process the attached activation file, the authorization file you copied is renamed with a .rejected extension and the utility logs an event with more details in the Windows Event Viewer's Application Log.

Starting the console

To start the console

1. Click **Start | Programs | LANDesk | LANDesk Management Suite**. (The actual program name may be different depending on the LANDesk product you've installed and the license used to activate your core server.)
2. Enter a valid user name and password.

If you're connecting to a remote core server, follow the normal Windows rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

3. Select the core server you want to connect to. The user must have proper authentication credentials to that core server.
4. Click **OK**.

The console opens with the layout (size, position, open tool windows, etc.) that was being used the last time this user logged out.

For additional consoles, the credentials you use to log into Management Suite must match the credentials used for any drives you have mapped to the core server. Otherwise, you might see a "Multiple connections" error in the console login dialog.

If you're running an additional console and have a drive mapped to the core server, you must u

About the Login dialog

Use this dialog to launch the console and connect to a core server.

- **Username:** Identifies a LANDesk user. This might be an administrator user or some other type of user with restricted access (see Using role-based administration). The user must be a member of the LANDesk Management Suite group on the core server. Follow the normal Windows NT rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).
- **Password:** The user's password.

Note: If a LANDesk Administrator changes the password of another user (i.e., an additional console user), the new password does not take affect until that user reboots their console. At that point, the user would enter their new password to log into the console.

- **Core server:** Specifies the core server you want to connect to. This drop-down list is the same as the core server drop-down list available on the console toolbar.

Changing the core server connection

The console lets you view and manage the contents of any database associated with a core server that you can connect to on your network. This allows you to create databases for different sites, organizational units, or logical internal networks.

You can only be connected to one core server at a time.

To change core server connections

1. Select a core server from the **Core** drop-down list located on the console toolbar. Or, enter a core server name in the text box and press **Enter**.

The server is searched for on your network. If found, you're prompted to log in at the standard Login dialog.

2. Enter a valid user name and password.

Follow the normal Windows NT rules for remote login (i.e., if the user is local to that core server, just enter the user name; if the user is a domain user, enter the domain name\user name).

Once you've connected to a core server, its name is automatically added to the **Core** drop-down list in the toolbar.

Role-based administration help

About the user properties dialog

Use this dialog to specify the selected user's rights, e-mail address, and scope. You can also see what groups or organizational units (OUs) the user is a member of. For more information, see [Using role-based administration](#).

Rights

Use this page to specify the user's rights. For more information, see [Understanding rights](#).

- **Assigned rights:** Specifies the rights of the user.

User

Use this page to specify the user's e-mail address. For more information, see [E-mailing reports](#).

- **E-mail:** Specifies the user's e-mail address.

Scopes

Use this page to specify the user's scope. For more information, see [Creating scopes](#).

- **Assigned scopes:** Specifies the scopes the user is assigned to.
- **Add:** Enables you to add the user to additional scopes.
- **Remove:** Removes the selected scope from the user, so the user is no longer assigned to that scope.
- **New:** Enables you to create a scope.
- **Edit:** Enables you to edit the selected scope.

Member of

Use this page to see what groups or OUs the user is a member of. For more information, see [Role-based administration overview](#).

- **Member of:** Specifies the groups the selected user belongs to.

About the group and OU Properties dialog

Use this dialog to specify the rights of the selected group or organizational unit (OU). You can also see what other groups or OUs it is a member of. For more information, see [Using role-based administration](#).

Rights

Use this page to specify the rights of the group or OU. For more information, see [Understanding rights](#).

- **Assigned rights:** Specifies the rights of the group or OU.

Member of

Use this page to see what groups or OUs the selected group or OU is a member of. For more information, see Role-based administration overview.

- **Member of:** Specifies the groups or OUs the selected group belongs to.

About the Scope Properties dialog

Use this dialog to configure the scope's properties. For more information, see Creating scopes.

- **Scope name:** Specifies the name of the scope.
- **Select a scope type:** Specifies what the scope applies to. The scope type determines what definitions can be applied to the scope.
- **New:** Enables you to create a scope definition based on the selected scope type.
- **Definition:** Displays the parameters that determine what the scope applies to.
- **Device group filters:** Lists any filters that affect the scope.
- **Edit:** Enables you to edit the scope's definition.

About the Login to Active Directory dialog

Use this dialog to access your active directory, so you can add groups and organization units (OUs) to the application. Then you'll be able to assign them rights and add them to other groups.

- **LDAP:** Specifies the path to the LDAP directory in order to access the groups and OUs (see Using LDAP directories).
- **User name:** Specifies the user name to authenticate to the server.
- **Password:** Specifies the password to authenticate to the server.

About the Available Active Directory Groups and OUs dialog

Use this dialog to add groups and organizational units (OUs) to your **Active Directory** folder. These groups can be assigned rights and added to other groups. When users become a member of a group or OU, they inherit the rights of the parent node in addition to their own. A user's individual rights may allow access to functionality beyond the rights granted by the group or OU. Otherwise, they'll assume the same rights as the group or OU they belong to. For more information, see Using role-based administration.

Managed device help

The **Agent configuration** window (**Tools | Configuration | Agent configuration**) is where you customize device agent configurations. Use the **Agent configuration** dialog to specify the agents you want to install and the options for those agents. You can create as many agent configurations as you want. Only one configuration can be the default. You can use this window to create Windows, Macintosh, Linux, and server agent configurations

To create a configuration

1. Click **Tools | Configuration | Agent configuration**.
2. Click the **New** button to create a new Windows configuration. Click the **New Mac** button to create a new Macintosh configuration.
3. Complete the **Agent configuration** dialog as described in the following sections. Click **Help** on a page for more information.

Note: If you use the **Agent configuration** dialog to create a new default agent configuration, be aware that all devices who are configured by WSCFG32 using login scripts will be automatically reconfigured with the new default configuration settings the next time they log in, even if their current settings match the new default settings.

The following sections describe the **Agent configuration** dialog pages.

About the Agent configuration dialog's Start page

The **Agent configuration** dialog's **Start** page contains the following options:

- **Configuration name:** This option appears above all dialog pages. Enter a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears in the **Agent configuration** window.
- **Default configuration:** Shows whether this configuration is the default configuration that gets installed. The only way to change this option is by clicking **Set as default** from the configuration's shortcut menu.
- **Standard LANDesk agent:** Installs the standard LANDesk agent that forms the basis of communication between devices and the core server. This option is required. You can't disable it, but you can customize the components associated with it.
- **Custom data forms:** Presents a form to users for them to complete. You can query the core database for the data users enter. Use this to retrieve customized information from users directly.
- **Remote control:** Lets you take control of a device or server from across the network. Minimizes the time it takes to resolve customer issues from a centralized help desk. Use this to provide remote management of devices across the LAN/WAN.
- **Software distribution:** Automates the process of installing software applications or distributing files to devices. Use this to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.
- **Profile migration:** Doesn't install a separate agent on devices; but ensures that the necessary LANDesk agency is present on managed devices in order for them to be capable of capturing and migrating user profiles.

- **LANDesk Trust Agent:** Installs the LANDesk Trust Agent (LTA) on managed devices, which allows the device to communicate with the LANDesk DHCP server and posture validation server. A trust agent is required in order to use either of the two LANDesk trusted access solutions that enables compliance security scanning and remediation. (**Note:** If you've implemented the LANDesk DHCP trusted access solution, you can use an agent configuration to install the LANDesk Trust Agent (LTA) on managed devices. If you've implemented the Cisco NAC trusted access solution, you must manually install the Cisco Trust Agent (CTA) on managed devices. Keep in mind that in order to provide additional device management capabilities, you can also install the LTA (which includes the inventory scanner and local scheduler) on managed devices even if you're using the Cisco NAC solution. In other words, you can have both trust agents installed on the device. However, if you're using the LANDesk DHCP solution, you should not install the CTA on managed devices.)
- **Select all:** Selects all available agents in the **Agents to install** list.
- **Clear all:** Clears all available agents in the **Agents to install** list, except for **Standard LANDesk agent**, which is mandatory.
- **Defaults:** Selects all agents in the **Agents to install** list, except for **LANDesk Trust Agent**.
- **Perform full inventory scan during installation:** When this configuration is installed on clients, whether to do a full inventory scan during the agent installation. The default is checked.
- **Temporary install directory:** Specifies the temporary folder used on managed devices during agent installation. This folder must be writeable for agent installation to succeed.

Deploying the standard LANDesk agent (includes the inventory scanner, local scheduler, and security scanner)

All Management Suite components require the standard LANDesk agent (formerly known as CBA), which is installed by default on all device installations. Among other things, the standard LANDesk agent provides device discovery and manages core server/device communication.

Use the Standard LANDesk agent pages to configure the Standard LANDesk agent, which includes these components and settings:

- Inventory scanner
- Local scheduler
- Bandwidth detection
- Device reboot options

About the Agent configuration dialog's Standard LANDesk agent page

Use this page to configure certificate-based security and what scope devices using this configuration will have.

Trusted certificates

Select the core server certificates you want devices to accept. Devices will only communicate with cores and consoles they have certificates for. For more information on certificates and copying them from other core servers so you can select them here, see "Agent security and trusted certificates."

Scope

If you want devices to be included in scopes that are based on custom directories, enter a directory path in the **Path** field. The path you enter here defines the device's computer location inventory attribute. Scopes are used by Management Suite's role-based administration to control user access to devices, and can be based on this custom directory path.

Custom directory paths use a format that's similar to a file path, but with forward slashes as separators. If you want to use custom directory-based scopes, first decide how you want to categorize your devices for role-based administration. You might do categorize devices by geographic locale, department or group name, or any other organizational detail you prefer.

Directory paths you enter here as part of an agent configuration are added to a device's registry under:

```
HKLM\Software\Intel\LANDesk\Inventory\ComputerLocation
```

You don't have to fill in this field. If you leave it blank, the device's computer location attribute is defined by its Active Directory or eDirectory path.

When the inventory scanner is run on a device, it records the device's computer location inventory attribute. If you entered a custom directory path in the **Path** field, that path is the directory the scanner records. If you left the custom directory path blank, the scanner tries to populate the computer location inventory attribute with the device's Active Directory or NetWare eDirectory path. If neither a custom directory path or an LDAP-compliant directory is found, the computer location attribute isn't defined. However, the device can still be accounted for in both query scopes or device group scopes.

For more information on how scopes are used in Management Suite's role-based administration, and how you can define a scope using custom directory paths, see [Using role-based administration](#).

About the Agent configuration dialog's Inventory scanner page (under standard LANDesk agent)

The **Agent configuration** dialog's **Inventory scanner** page contains the following features:

- **Manual update:** The software list used to exclude titles during software scans is loaded down to each remote device. Each time the software list is changed from the console, you must manually resend it to remote devices.
- **Automatic update:** Remote devices read the software list from the core server during software scans. If this option is set, each device must have a drive mapped to the LDLOGON directory on the core server so they can access the software list. Changes to the software list are immediately available to devices.
 - **Update using HTTP:** Beginning with Management Suite 8, the inventory scanner can use HTTP for LDAPPL3.INI file transfers. This allows the scanner to support Targeted Multicast features like polite bandwidth and peer download. Peer download allows devices needing LDAPPL3.INI updates to check with the core server for the latest version's date, then broadcast to peers on their subnet to see if a peer has the update in its multicast cache. If a peer has the update, the file transfer happens on the local subnet without generating network traffic across routers or WAN links.
- **Start inventory scan:** Determines when the inventory scanner runs on devices with this agent configuration. You can select one or more of the start options: **IP address change**, **At startup using the run key registry setting**, and **Frequency** (uses the local scheduler to run the inventory scanner on a recurring basis, at the earliest opportunity within the hourly range of the recurring time period you specify).

About the Agent configuration dialog's Local scheduler page (under standard LANDesk agent)

The local scheduler agent enables Management Suite to launch device tasks based on a time of day or bandwidth availability. The local scheduler agent is most useful for mobile computers that may not always be on the network or may connect to the network via a dialup connection. For example, you can use the local scheduler to allow mobile computer package distribution only when those devices are on the WAN.

When you schedule software packages for distribution, or when you create application policies, you can specify which bandwidth the packages or policies require before they are applied.

The local scheduler runs as a service on Windows NT/2000/XP, or as a pseudo-service on Windows 95/98.

The **Local scheduler** page contains the following features:

- **Enter the frequency that the agent polls for tasks:** How often the local scheduler checks for tasks. The default is 30 seconds. The polling interval you select is stored on the local computer.
- **Bandwidth detection interval:** How often the local scheduler should check bandwidth. The default is 120 seconds. Bandwidth checks happen only when there's a pending scheduled task.

About the Agent configuration dialog's Bandwidth detection page (under standard LANDesk agent)

Bandwidth detection enables bandwidth detection between devices and the core server. You can limit Management Suite actions such as software distribution based on available bandwidth. Use this option if you have remote devices or devices that connect to the network via a slow link.

The **Agent configuration** dialog's **Bandwidth detection** page contains the following features:

- **Choose bandwidth detection method:** Select whether to use ICMP or PDS for bandwidth detection. ICMP sends ICMP echo requests of varying sizes to the remote device and uses the round trip time of these echo requests/responses to determine the approximate bandwidth. ICMP also distinguishes between LAN (high speed) and WAN (slow, but not dialup) connections. However, not all routers or devices support ICMP echo requests.
If your network isn't configured to allow ICMP echo requests, you can select PDS. The PDS bandwidth tests aren't as detailed, but they detect either a LAN or a low-bandwidth RAS (typically dialup) connection. The PDS method only works if the PDS service is running on the package server. You can install this service by deploying the standard LANDesk agent to the package server.
- **LAN threshold, in bits per second:** The threshold that classifies a connection as WAN rather than LAN. The default is 262144 bps.
- **Enable dynamic bandwidth throttling:** Specifies that the network traffic a device creates has priority over distribution traffic. This option also forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted.
This option is also available from the **Delivery methods** dialog. If you enable this option in agent configuration but not in the **Delivery methods** dialog, it will still be enabled on the device. If you don't enable this option in agent configuration but do enable it in the **Delivery methods** dialog, dynamic bandwidth throttling will be enabled on the device for that package script.

About the Agent configuration dialog's Device reboot options page (under standard LANDesk agent)

Once you install Management Suite agents on devices, they may need a reboot to complete the agent configuration. The **Agent configuration** dialog's **Device reboot options** page contains the following features:

- **Do not reboot devices after configuration:** Devices won't reboot, even if the selected components require a reboot. If a reboot is necessary, components won't work correctly until the device reboots.
- **Reboot devices if necessary:** Reboots devices only if a selected component requires a reboot.
- **Reboot with user option to cancel:** If a selected agent requires a reboot, users will have the option to cancel the reboot. If a reboot is necessary, components won't work correctly until the device reboots. You can select how long the reboot prompt stays on the user's screen before the computer reboots. This timeout is useful for users that are away from their computers when the device deployment happens.
- **Allow user to cancel reboot within this time period:** If you want to give users a chance to cancel the reboot before it happens automatically, enter how long you want the reboot prompt to appear.

Deploying custom data forms

You can create and distribute custom data forms to collect device information that will supplement the standard information available in the core database. The forms you create using the Form Designer can be distributed by a device deployment service or by using the **Agent configuration** dialog.

Customize the forms that are distributed to devices in your management domain using the form designer. For more information, see "Using custom data forms."

About the Agent configuration dialog's Custom data forms pages

The custom data forms section consists of two pages. The **Custom data forms** page contains the following features:

- **Manual update forms:** Selected forms are sent to each device. If the forms change or new forms are added, you must manually resend the forms to remote devices.
- **Automatic update:** Remote devices check the core server for updated forms each time the inventory scanner is run, such as at startup. Each device must have a drive mapped to the LDLOGON directory on the core server to access the updated forms.
- **Display forms to end user:** Choose how remote devices access custom forms:
 - **On startup:** The selected forms run automatically at startup on each device.
 - **When inventory scanner runs:** The selected forms run only when the inventory scanner is run on each device. The inventory scanner runs automatically on startup, and can be run manually by devices at any time.
 - **When launched from the LANDesk program folder:** The selected forms appear as items in the device's LANDesk Management folder. They aren't automatically run.

The **Forms sent with agent** page lists all defined custom data forms. Mark which forms are made available to devices receiving this configuration task. You'll have to create forms (**Tools | Configuration | Custom Data Forms**) before they can appear in this list.

Deploying software distribution

Software distribution automates the process of installing software applications and distributing files to devices. Use this agent to install applications simultaneously to multiple devices or to update files or drivers on multiple devices.

Software distribution uses a Web or file server to store packages. Devices access this package server when downloading a package. You'll need to configure a package server as described in the software distribution chapter in the *User's Guide*. You can deploy the software distribution agent to devices before you set up a package server. For more information, see "Distributing software and files."

About the Agent configuration dialog's Software distribution page

The **Agent configuration** dialog's **Software distribution** page contains the following features:

- **TCP port number:** Specifies the port the policy-based management agent will use to communicate with the core server. The default port is 12176. You'll need to make sure this port is open on any firewalls between devices and the core server. If you change this port, you'll also need to change it on the core server. You can change the port the QIP server service uses by editing this registry key:

HKLM\Software\Intel\LANDesk\LDWM\QIPsrvr

About the Agent configuration dialog's Logon policies page (Under software distribution)

The policy-based distribution agent enables you to automatically install sets of applications on groups of devices. Use this agent to manage groups of devices that have common software needs. For more information, see "Using policy-based distributions."

In order for devices to receive policies that are targeted through Active Directory or NetWare Directory Services, they have to be configured to log in to the directory. This means that they need to have all the correct device software installed, and they need to actually log in to the correct directory so that their fully distinguished name will match the name that was targeted through Directory Manager.

Windows 95/98 devices need to be configured to log in to the domain where the Active Directory resides. Windows NT and Windows 95/98 don't include Active Directory support. You must install Active Directory support on devices that log in to a directory and require Application Policy Management. As of this printing, more information on installing Active Directory device support was available here:

<http://www.microsoft.com/technet/archive/ntwrkstn/downloads/utlis/dsclient.msp>

The Policy-based deployment page has two tabs that configure how the policy-based agent works. You can have the agent launch at startup (the **Logon policies** page) and/or periodically through the local scheduler (the **Local scheduler policies** page). For each launch method, you can configure how the agent works.

The **Agent configuration** dialog's **Logon policies** pages contain the following features:

- **Enable:** Enables policy-based distribution on devices
- **Run policy-based agent silently:** Runs without showing its interface on the device.
- **Run required policies and cache the rest:** Runs required policies. Caches preferred and optional policies locally in case devices want to install policies later.
- **Only run policies from the device's local cache:** Runs policies from the local cache only. Devices won't initiate any network traffic.
- **Agent timeout:** (logon only) How long the pull delivery window will stay open on a device if a user doesn't close it. You can set the timeout in seconds.

About the Agent configuration dialog's Local scheduler policies page (under software distribution)

Use the **Local scheduler policies** page to configure policies so they run more frequently than just at logon.

- **Enable:** Allows the local scheduler to run policies.
- **Run policy-based agent silently:** Runs without showing its interface on the device.
- **Run on IP address change:** If the local scheduler agent detects a client IP address change, the policy-based agent will run.
- **Run required policies and cache the rest:** Runs required policies. Caches preferred and optional policies locally in case devices want to install policies later.
- **Only run policies from the device's local cache:** Runs policies from the local cache only. Devices won't initiate any network traffic.
- **Only run policy-based agent when a user is logged in:** Runs policies when a user is logged in.
- **Frequency:** When the local scheduler should launch the policy-based agent on devices.

Deploying remote control

When deploying remote control, you need to consider which security model you want to use. You have these choices:

- **Local template:** This is the most basic security that uses whatever remote control settings are specified on the device. This model doesn't require any other authentication or group membership.
- **Windows NT security/local template:** This security model uses a Windows NT Remote Control Operators group. Members of this group are allowed to remote control devices. Permitted users still use the device's remote control settings, such as permission required.
- **Certificate-based/local template:** This is the most secure option and is new to Management Suite 8. It's also known as on-demand secure remote control and is described in the next section.

About on-demand secure remote control

LANDesk Management Suite 8 introduces a new on-demand secure remote control (certificate-based/local template) that you can use. This new remote control improves on the prior version in these ways:

- Remote consoles authenticate with the core server.

- The remote control agent on a device loads on-demand once a remote control session is authorized by the core.
- All remote control authentication and traffic is encrypted over an SSL connection.
- Once remote control finishes with a device, the remote control agent unloads.

Here's an outline of the remote control communication flow:

1. The Management Suite console asks the core server for permission to remote control the specified device.
2. If the console/user is authorized to remote control the specified device, the core server tells the device to load the remote control agent with a randomly generated set of authentication credentials.
3. The core server passes the authentication credentials to the console.
4. The console authenticates to the device with the authentication credentials and remote control begins.

Warning: On-demand remote control requires the core server

With on-demand remote control, if the core server isn't available, consoles won't be able to remote control devices. On-demand remote control requires the core server to work.

Using Windows NT security/local template with Windows XP devices

For Windows NT security/local template authentication to work with Windows XP devices, you must configure devices so that the Windows XP sharing and security model for local accounts is classic (local users authenticate as themselves). If you don't do this, the default guest-only authentication won't work with remote control's Windows NT security.

To set the Windows XP security model to classic

1. On the Windows XP device, click **Start | Control Panel**.
2. In the **Administrative Tools, Local Security Policy** applet, click **Security Options | Network access: Sharing and security model for local accounts**, and set it to **Classic - local users authenticate as themselves**.

About the Agent configuration dialog's Remote control page

The **Agent configuration** dialog's **Remote control** page contains the following features:

- **Local template:** Uses only the local device simple permissions and authentication set from the Remote Control Settings page of this wizard.
- **Windows NT security/local template:** Only allows members of the Remote Control Operators group to initiate remote control connections from the console to remote devices. Permitted users are still required to use the permissions set from the Remote Control Settings page of this wizard.
Since the Remote Control Operators group is a local group, each device has its own copy of the group. To avoid managing each device's Remote Control Operators group individually, include global (domain level) groups with each local group. Permitted users still use the device's remote control settings, such as permission required.

- **Certificate-based\local template:** Communication between the console and remote devices is authenticated using the core server; only consoles authenticated from the same core server can use remote control functions for these devices. Select the certificates you want to allow in the Trusted Certificates list. Permitted users are still required to use the permissions set from the **Permissions page**. This option is also known as on-demand secure remote control, as described earlier in this chapter.

Adding users to the Remote control operators group and the View only group

If you select **Windows NT security/local template** as your security model, the **Remote control operators group** and **View only group** boxes list the users for the console or for the selected Windows NT domain. The users you select here will have remote control access to the devices that receive the settings defined in this configuration settings file. **View only group** users can only view remote devices. They can't take over the mouse or keyboard.

When adding users to one of the remote control groups, the console uses the logged-on user's Windows credentials, not the LANDesk console user's credentials, to list the users in a domain. If the **List users from** box isn't showing the domain you want, log in to Windows as a user with rights on that domain.

To choose from an existing server or domain

1. In the **Remote control** page, click **Windows NT security/local template** and click the **Add** button.
2. In the **List names from** box, select either the core server name or a Windows NT domain name containing user accounts.
3. In the user list, select one or more users and click **Insert** to add them to the **Inserted names** list.
4. Click **OK** to add the selected names to the Remote Control Operators group on each device that receives these configuration settings.
5. If you want any of these users to be in the **View only group**, select them and move them over. Users can only be in one group.

To manually enter names

You can enter names manually by clicking in the **Inserted names** list and using any of the following formats to enter names. Use semicolons to separate names.

- **DOMAIN\username** where DOMAIN is the name of any domain accessible to the target device.
- **MACHINE\username** where MACHINE is the name of any device in the same domain as the target device.
- **DOMAIN\groupname** where DOMAIN is the name of any domain accessible to the target device, and groupname is the name of a management group in that domain.
- **MACHINE\groupname** where MACHINE is the name of any device in the same domain as the managed node, and groupname is the name of a management group on that device.

If you don't specify a domain or device name, it is assumed that the user or group specified belongs to the local device.

Click **OK** to add the names to the Remote Control Operators user group on the target device.

About the client setup dialog's Permissions page (under remote control)

The **Remote control** section's **Permissions** page contains the following features:

- **Remote control:** Grants permission to control the device.
- **Reboot:** Grants permission to reboot the device.
- **Chat:** Grants permission to chat with the device.
- **File transfer:** Grants permission to transfer files to and from the device's local drives.
- **Run programs on remote device:** Grants permission to run programs on the device.

You can also specify these remote control settings:

- **Permission required:** Requires the console user to receive permission from the device before any kind of remote access is granted.
 - **Only when the user is logged on:** Prompts the user currently logged on for permission. If nobody is logged on, remote control doesn't require permission.
 - **Ask for all permissions at once:** Prompts user once for session permissions. Normally with permission required, the user has to permit remote control, chat, file transfer, and so on individually. This option gives permission for all remote control-related options for the duration of a session.
 - **View only:** Remote control operators can only view the device, they can't interact with it remotely.

About the Indicators page (under remote control)

The **Remote control** section's **Indicators** page contains the following features:

- **Floating desktop icon:** Displays the remote control agent icon on the device screen at all times or only when being remotely controlled. When being controlled by the console, the icon changes to show a magnifying glass and the icon's title bar turns red.
- **System tray icon:** Places the remote control agent icon in the system tray. Again, the icon can be visible all the time or only while being remotely controlled.

When using certificate-based remote control security, the indicator is only visible during remote control. This security model unloads the remote control agent and the indicator icon when remote control isn't being used.

Deploying and configuring the security and patch scanner

The security and patch scanner agent is installed by default along with the standard LANDesk agent. When creating device agent configurations, you can configure certain aspects of when and how the security scanner runs on managed devices, as well as enable and configure frequent security scans, and spyware and application blocking.

The security scanner allows you to scan managed devices for vulnerabilities and other security risks; such as spyware, unauthorized applications, software and driver updates, system configuration security threats, custom security definitions, and more. The content of your security scan depends on your Security Suite content subscription and which security type definitions you've downloaded with the Security and Patch Manager tool. You can also remediate detected problems via repair tasks and policies. For more information, see Using Security and Patch Manager in the *Users Guide*.

About the Agent configuration dialog's Security and patch scan page

Use this page to configure whether the security scanner is launched automatically (by device login, by the local scheduler, or by IP address change) on managed devices with this agent configuration, and to configure other security scanner options. You can also run security scans as scheduled tasks and policies from the console, or manually at a managed device.

This page contains the following options:

- **During login using the Run key registry setting:** Places the security scanner in the Windows registry's run key which causes the scanner to launch whenever a login occurs on devices with this agent configuration.
- **Frequency:** Enables the local scheduler to automatically launch the security scanner on devices with this agent configuration. This option lets you run a security scan on a recurring basis, at the earliest opportunity within the time period you specify. The **Launch only when a user is logged in** option lets you control whether the security scanner runs at the specified frequency whether or not a user is logged in to the managed device.
- **IP address change:** Forces a security scan whenever the IP address changes on devices with this agent configuration. For example, if a mobile device with an agent configuration that has this option enabled connects to another network and then attempts to reconnect to your network with a different IP address, the security scanner runs automatically.
(Note: All security scanner launch options can be selected concurrently.)
- **Global settings:** Applies to all devices with this agent configuration, overriding task-specific settings.
 - **Never reboot:** Ensures devices with this agent configuration won't reboot when the security and patch scanner is running. This is a global setting for all devices with this agent configuration, which means it overrides any end user reboot settings that are applied to either a security scan or repair task. In other words, regardless of the end user reboot settings used by a security task, this global setting will take precedence. Check this option if you know you don't want devices to reboot during any security and patch scanner operation, and leave it clear if you want to be able to configure the reboot options with the Security and patch manager tool.
 - **Never auto fix:** Ensures devices with this agent configuration won't allow a security and patch scan to perform an auto fix when remediating detected vulnerabilities, even if the vulnerability has auto-fix enabled. As a global setting for all devices with this agent configuration, this setting overrides any end user auto-fix setting you've applied to a security scan task. Use this setting if you want to guarantee devices can't have detected vulnerabilities automatically remediated by a security scan.
- **Scan and repair settings:** Determines the display, end user interaction, reboot, and content settings for the security scanner when it is launched by the method(s) selected above specific to this agent configuration. Select a scan and repair setting from the drop-down list, or click **Configure** to edit an existing setting or to create a new one.

About the Client Setup Utility dialog

The **Agent configuration utility** dialog displays the status of a scheduled device configuration task as the task is processed. This dialog is for information only; the devices to be configured were selected when the task was scheduled.

The **Agent configuration utility** dialog contains the following features:

- **Clients to configure:** Lists the devices scheduled to receive these configuration settings.
- **Clients being configured:** Lists the devices that have been contacted by the console and are in the process of being configured with this settings file.
- **Clients completed:** Lists the devices that the console has configured during this scheduled session. If the configuration attempt was successful, the status is Complete. If the configuration attempt failed for any reason, the status is Failed. These statuses are mirrored in the Scheduled Tasks window when this task is selected.
- **Creating configuration files:** Displays a status bar indicating the completion status of the entire configuration task.

Deploying to NetWare servers

You can install the inventory scanner to NetWare servers. The NetWare agent configuration utility will modify the AUTOEXEC.NCF to load the scanner on startup. You must have the NetWare client loaded on the console you're installing the agent from and you must have write access to the NetWare server you want to install the agents on.

To install remote control and inventory on a NetWare server

1. In the Management Suite console, click **Configure | Deploy LDMS client to NetWare server**.
2. Enter the NetWare server name. Click **Install**, and then click **OK**. This installs the agents to the NetWare server.

Deploying to Linux servers

You can use the console's agent configuration tool to deploy agents to these Linux versions:

- Red Hat Linux 7.3, 8.0, and 9
- Red Hat Linux Enterprise 3
- SuSE Linux 9.1

For more information on Linux agent deployment, see *Configuring Linux and UNIX device agents*.

About the Start page (under Linux Agent configuration)

The Linux **Agent configuration's Start** page has these options:

- **Configuration name:** Enter a name that describes the configuration you're working on. This can be an existing configuration name or a new one. This name appears in the **Agent configuration** window.
- **Standard LANDesk agent, Remote control, and Software distribution:** These options install by default and you can't disable them.

- **LANDesk vulnerability scanner:** Installs the Linux version of the vulnerability scanner. The scanner only reports on problems, it doesn't remediate them.
- **Defaults:** Resets the options to default (disables the **LANDesk vulnerability scanner** option).

About the Standard LANDesk agent page (Under Linux Agent configuration)

The Linux **Agent configuration**'s **Standard LANDesk agent** page has these options:

- **Trusted certificates for agent authentication:** certificates control which core servers can manage devices. Check the core server certificates that you want installed with this configuration. For more information, see Agent security and trusted certificates.
- The other options on this page are dimmed and don't apply to Linux agent configurations.

About the Inventory scanner page (Under Linux Agent configuration)

The Linux **Agent configuration**'s **Inventory scanner** page has these options:

- **Start inventory scan:** You can select **Daily, Weekly, or Monthly**. The option you select adds a command to the server's cron.daily, cron.weekly, or cron.monthly file that runs the inventory scanner.

Inventory help

About the Inventory window

Use the **Inventory** window to view a device's complete inventory, including the following components:

- **BIOS:** Type, date, ID bytes, manufacturer, ROM version, SMBIOS version, and system model for the BIOS. The BIOS permanently resides in the computer's ROM (read-only memory) and enables the computer's memory, disk drives, and monitor to communicate.

Additional BIOS information appears in the Inventory window as BIOS text strings. To view and search BIOS text strings, expand the **BIOS** object, select **BIOS Strings**, right-click the **Data** attribute and select **Properties**, and then click **Extended Values**. During an inventory scan, the available text strings are exported to the BIOS to a text file, LDBIOS.TXT. You can set up a query in the LDAPPL3.INI file that outputs one or more of the BIOS text strings to the console. For more information, see Additional inventory operations and troubleshooting.

- **Bus:** Bus type. The bus connects the microprocessor, disk drives, memory, and input/output ports. Bus types can be ISA, EISA, VESA Local Bus, PCI, and USB.
- **Coprocessor:** Type of coprocessor, if present. The coprocessor is distinct from the main microprocessor, though it can reside on the same motherboard or even the same chip. The math coprocessor evaluates floating point operations for the main microprocessor.
- **Environment:** File locations, command path, system prompt, and other variables for the Windows environment.
- **Keyboard:** Keyboard type attached to the device. Currently, the most common type of keyboard is the IBM-enhanced keyboard. Code page is the language the keyboard uses.
- **LANDesk Management:** Information about the agents, client manager, and Alert Management System (AMS). Also contains information about the inventory scanner and initialization files.
- **Mass Storage:** Storage devices on the computer, including floppy drives, hard disks, logical and tape drives, and CD-ROM. The hard disk and floppy drive objects include head, number, sector, and total storage attributes.
- **Memory:** Page file, physical, and virtual memory attributes. Each of these memory objects includes byte attributes. The first byte is the amount of memory available. The second byte is the total memory.
- **Mouse:** Type of mouse attached to the device. Mouse type values include PS/2, serial, and infrared.
- **Network:** Network adapter, NIC address, and the adapter's node address information. The Network object includes information for each protocol loaded on the computer. Typical values include IPX*, NetBEUI, NetBIOS, and TCP/IP objects.
 - **IPX** is a protocol that NetWare* servers can use to communicate with their devices and other servers. The IPX object contains the address, network number, and node address attributes.
 - **NetBEUI** allows a computer to communicate with Windows NT/2000, Windows for Workgroups, or LAN Manager servers. Microsoft now recommends using TCP/IP for these connections.
 - **NetBIOS** is an interface (API) for applications to send and receive packets to each other over TCP/IP, NetBEUI, or IPX.

- **TCP/IP** is a protocol that enables a computer to communicate over the Internet and with WANs. This object contains the address (contains the computers TCP/IP address), host name (contains the computers DNS context), IP routing enabled, and NetBIOS resolution (uses DNS and WINS proxy enabled attributes).
- **Network Adapters:** Attributes for every installed network adapter on the device.
- **OS:** Operating system, drivers, services, and ports. These objects and their attributes vary according to the configurations of the loaded drivers and services.
- **Ports:** Objects for each of the computers output ports (serial and parallel). Each output port contains address and name attributes. The address attribute contains the hardware address for the port.
- **Printers:** Objects for each printer connected to the computer, either directly or through a network. The printer objects contain driver, name, number, and port attributes. The port attribute contains either the network queue or the port the printer is connected to.
- **Processor:** Attributes of the device's CPU. Detects Intel, Motorola 680x0, and PowerPC processors.
- **Resources:** Objects for every hardware resource of the computer. Each hardware resource object contains attributes that describe the type of resource and any ports and interrupts it is using.
- **Software:** Objects for every software application installed on the device's hard drive. Each software program object lists attributes that typically contain the software name, location, and version number.
- **Video:** Objects for each video adapter on the device. The video adapter object typically contains attributes that describe the resolution and the number of supported colors.

About the Inventory attribute properties dialog

Use this dialog to view an attribute's properties. The **Characteristics** tab displays the following information:

- **Name:** The name of the core database attribute whose properties you're viewing.
- **Value:** The value assigned to this inventory attribute.
- **User defined:** Indicates whether the selected attribute was defined by the user or not. This option can't be changed.
- **Primary key:** Indicates whether the attribute uniquely identifies objects of the same type. An object can have only one primary key.
- **Notify event log on change:** Whether a change to this attribute should be logged to the Windows event log.
- **Track changes in database history:** Whether changes to this attribute should be logged to the inventory history log.
- **Generate AMS alert:** Whether changes to this attribute should be sent to AMS to generate an alert.
- **Event log/alert severity:** The severity of a log or alert entry.
- **Factor (Integer values only):** Integer value used to divide the attribute into units. If you change the factor value, you must enter the appropriate code in the format specifier field. For example, to view the number of Megabytes if the attribute is recorded in Kilobytes, enter the value 1000.

- **Format specifier (Integer values only):** Notation used to display the value in appropriate form. For example, %d MB displays the attribute value without decimal values; %.1f MB displays the attribute value to the first floating decimal point in MB units. If no factor value is entered, this format specifier must describe integer values (%d, %u, etc). If a factor value is entered, this format specifier must describe floating point values (%f, %e, etc).

About the Inventory change settings dialog

Use this dialog to select which inventory attributes are logged when changes occur at individual devices, and to determine where those changes are logged.

- **Current inventory:** Lists all objects stored in the core database. Click an object to display its attributes in the Log event in list. Expand an object group to see the data objects contained within it.
- **Log event in:** Lists the attributes of the inventory object selected in the Current inventory list.

To set where inventory changes are logged, select an attribute and check one or more options. Check the **Inventory** option to log inventory changes in the device's **Inventory changes history** dialog. Check the **NT Log** option to log inventory changes in the Windows NT event log. Check the **AMS** option to send inventory changes as an alert via AMS (configure AMS alerts with the Alert Settings tool).

- **Log/Alert severity:** Lists the alert priority options. This feature is dimmed until an attribute is actually selected. You can select a severity level of None, Information, Warning, or Critical.

About the Inventory changes history dialog

Use this dialog to view a device's inventory changes. You can also print and export the inventory changes history from this dialog.

- **Device Name:** Displays the name of the device(s) selected in the console's network view for which inventory change data is requested.
- **Component:** Identifies the system component that has changed. (Only components selected in the Inventory Change Settings dialog can appear here.)
- **Attribute:** Identifies the specific component attribute being logged.
- **Time:** Indicates when the change occurred.
- **New Value:** Shows the new (changed) value for the listed attribute.
- **Old Value:** Shows the old (previous) value for the listed attribute.
- **Print:** Opens a standard print dialog where you can print the contents of the inventory changes history.
- **Export:** Opens a Save As dialog where you choose a name and location for the exported .CSV file containing the inventory changes history.

You can click a column heading to sort the listing by that attribute. Click the heading again to reverse the sort order.

About the Create/Edit a Custom Data Form dialog

Custom data forms are not supported in LANDesk Security Suite

Custom data forms is not available with a LANDesk Security Suite only license. You must have a full LANDesk Management Suite license in order to use the custom data forms feature.

Use this dialog to create or edit a custom data form.

- **Form name:** Identifies the form and appears on the form viewer when a user fills out the form.
- **Description:** Provides additional information to users about the form.
- **Add:** Opens the **Add question** dialog where you can create a new question for the form.
- **Edit:** Opens the **Edit question** dialog where you can edit any of the question's options.
- **Delete:** Removes the question from the form.
- **Page break:** Controls the layout of the form by adding page breaks to group questions on pages. When there's a page break, users click the Next button to proceed to questions on the next page.

Note: The maximum number of questions per page is nine.

- **Preview:** Opens the form so that you can preview how it will look for users. In preview mode, you don't have to fill in any data and nothing you type is saved.

About the Add/Edit question dialog

Use this dialog to create or edit questions that appear on the custom data form. Forms consist of questions and a place for users to put their answers. First, identify the question:

- **Question text:** One-line description of what's being asked for. This text appears beside the data field.
- **Inventory Name:** Name of the database field in the core database. If you wanted to query the core database for this item, the label ID is what you would query on.
- **Description:** Additional information that appears when users click Help (or press F1) while in this question's data field.

You also need to specify what type of data field (control) to show beside each question, and if it is required. The available data fields are:

- **Edit box:** Users type their answer in an editable text box.
- **Combo box (edit list):** Users select one of the predefined list items, or type in a new one of their own.
- **Combo box (fixed list):** Users select one of the predefined list items.
- **Make the control a required field to fill out:** Forces the user to answer the question. The user can't finish a form or move to the next form page before responding to required fields.

About the Add items dialog

Use this dialog to add items to a drop-down list that the user can choose from when answering that question on a form.

- **Item name:** Identifies the item. This name appears in the question's drop-down list.
- **Items list:** Lists all the items that appear in the question's drop-down list.
- **Insert:** Places the item in the Items list.
- **Delete:** Removes the item from the Items list.

About the Select Multiple Forms to Distribute dialog

Use this dialog to create a group of forms that shows the group name and lists available forms that can be part of a group.

- **Name of group:** Identifies the group in the **Custom data forms** window.
- **Available forms:** Lists all of the available forms you can add to the group.
- **OK:** Saves the group and closes the dialog.
- **Cancel:** Closes the dialog without saving the group.

Reports help

About the Report Properties dialog

Use this dialog to configure your report. For more information, see [Creating custom reports](#).

- **Title:** Specifies the title of the report.
- **Description:** Provides a description of the report.
- **Query filter:** Specifies the query applied to the report.
- **Select:** Enables you to select an existing query, which provides the parameters for generating the report.
- **Edit:** Enables you to edit the query of the report.
- **New:** Enables you to create a custom query.
- **Chart type:** Specifies whether the report will include charting diagrams and information, as well as what type of chart to use.
- **Query field:** Specifies the parameter or query data that the chart will be based on.
- **Preview:** Generates and launches a preview of the report.
- **Design:** Launches the report designer, which enables you to customize your report and create report templates.
- **OK:** Saves the report and closes the dialog.
- **Cancel:** Closes the dialog without saving any changes.
- **Help:** Launches the help file.

About the Report published dialog

Use this dialog to perform the following tasks:

- **Report successfully published to:** Identifies the full path and file name of the published report. This is the network path of the file share that can be sent to viewers along with the LANDesk Report users name and password, in order to provide access to the published report. This field can't be edited.
- **Preview:** Opens the report in the appropriate application. An .HTML report opens in the default browser. If you don't have the appropriate application installed to access the file format, you can't preview the report from this dialog. For example, if the report is saved as a .PDF file, you won't be able to preview the report without a .PDF viewer like Adobe* Acrobat installed.
- **Copy path to clipboard:** Copies the full path and file name to the system clipboard for later pasting.
- **Close:** Closes the dialog.
- **Help:** Launches the help file.

About the Scheduled task - properties dialog

Use this dialog to select an owner for the task, schedule the publishing of the report, designate the destination of the report, and configure the SMTP server. For more information, see [Scheduling to publish a report](#).

Overview

Use this page to specify the owner of the task and to change the scheduled time of the task. This page summarizes the choices you've made in the dialog. If you want to modify any of your choices, click **Change** beside that choice.

- **Owner:** Specifies the owner of the task.
- **Show in common tasks:** Check this option if you want the task should show in the owner's common tasks folder.
- **Scheduled time:** Provides the schedule information of the task.
- **Change:** Takes you to the **Schedule task** page to reschedule the task.

Schedule task

Use this page to schedule the task. You can configure when the task runs and how retries should work.

- **Start time:** Specifies when to perform the task.
- **Leave unscheduled:** Leaves the task unscheduled, but retains the task.
- **Start now:** Initiates the task once the dialog is closed.
- **Start later:** Specifies the task to occur at a designated date and time.
 - **Date:** Specifies the date the task will occur.
 - **Time:** Specifies the time the task will occur.
- **Repeat every:** Check this option to specify the reoccurrence of the task based on the start time.

Recipients

Use this page to select the recipients of the report.

- **Name:** Check these options to specify where the report will be delivered.
- **Destination:** Provides the file path or e-mail address for where the report is delivered.
- **Reply e-mail:** Specifies a sender for e-mailed reports, which is the account that will receive reply e-mails.
- **Check all:** Selects all destinations.
- **Clear all:** Clears the selection of all destinations.

SMTP configuration

Use this page to configure the SMTP server.

- **Outgoing mail server (SMTP):** Specifies the SMTP server. Leaving <localhost> as your selection uses the default SMTP service on your core server.
- **Port number:** Specifies the port number for sending e-mail. The default port is 25.
- **This server requires a secure connection (SSL):** Check this option to specify if your SMTP server requires SSL.
- **My outgoing server (SMTP) requires authentication:** Check this option to specify if your SMTP server requires authentication.
- **Log on using NTLM authentication:** Specifies if your server uses NTLM for authentication.
- **Log on using:** Specifies whether your server uses a user name and password for authentication.

- **User name:** Provides the user name for authenticating to the SMTP server.
- **Password:** Provides the password for authenticating to the SMTP server.
- **Test e-mail:** Specifies an e-mail address that will receive a message verifying the SMTP server is set up correctly.
- **Test:** Sends the test e-mail to verify proper setup.

About the Report template properties dialog

Use this dialog to create a new report template. For more information, see [Creating a report template](#).

- **Title:** Enter a unique title for the report template.
- **Description:** Enter a description for the report template.

About the Report template dialog

Use this dialog to apply a report template. For more information, see [Applying a report template](#).

- **Report templates:** Lists the report templates that have been created.
- **Load:** Loads the selected report template and closes the dialog.
- **Delete:** Deletes the selected report template.
- **Rename:** Renames the selected report template.
- **Close:** Closes the dialog without applying any template.
- **Help:** Launches the help file.

About the New CSV report dialog

Use this dialog to create a .CSV report. For more information, see [Creating .CSV files](#).

- **File Name:** Enter a unique file name at the end of the existing path. If the directory path does not exist, you're prompted whether you want to create it.
- **Browse:** Enables you to browse to a file location.
- **Report on all devices:** Specifies the report to run on all devices, or only on currently selected devices in the network view.
- **Report on selected nodes:** Specifies the report to run on selected devices in the network view.
- **Current codepage encoding:** Causes the current codepage encoding to be used.
- **Unicode encoding:** Causes unicode encoding to be used.
- **OK:** Saves the report and closes the dialog.
- **Cancel:** Closes the dialog without saving the report.
- **Help:** Launches the help file.

About the Select Items dialog

This dialog enables you to specify your reporting criteria, which determines what information will be included in the report. By configuring these reporting parameters and narrowing your focus, you are able to produce more precise reports. In order to apply your reporting criteria, make your desired selections and click **OK**. For more information, see [Using reports](#).

Unmanaged Device Discovery help

About the Scanner Configuration dialog

Use the **Scanner configuration** dialog (**Tools | Configuration | Unmanaged device discovery, Scanner configuration** button) to customize and do unmanaged device scans.

- **Saved configurations:** Shows the saved scanner configurations. Save a configuration by changing the settings you want, clicking **New**, naming the configuration, and with your new configuration selected, clicking **Save**.
- **CBA discovery:** Discovers devices with the CBA agent running. If your devices have CBA, this is the fastest discovery method.
 - **PDS2 discovery:** Discovers devices using the older LANDesk PDS2 agent. You can only select this option if you select **CBA discovery** first.
- **Network scan:** Discovers devices using an ICMP ping sweep. This is the most thorough and slowest discovery method.
 - **IP FingerPrint:** Discovers device information where possible, such as OS type, logged in user, domain, and so on. Depending on the discovered device type and OS, UDD may find varying degrees of information. This option slows discovery somewhat, as UDD sends specially formed packets to discovered devices and analyzes the responses.
- **NT domain:** Discovers devices in a Windows NT domain. This option uses the NT domain account information and doesn't require an IP address range, though you can specify one. Selecting this option and clicking **Configure** shows the **NT domain configuration** dialog where you can customize the NT domain discovery settings.
- **Filter by IP range** (for both NT domain and LDAP): Filters NT domain and LDAP discovery by the IP ranges specified in **Starting IP** and **Ending IP**.
- **LDAP:** Discovers devices in an LDAP directory. Selecting this option and clicking **Configure** shows the **LDAP configuration** dialog where you can customize the LDAP discovery settings.
- **IPMI:** Looks for servers enabled with Intelligent Platform Management Interface, which allows you to access many features regardless of whether the server is turned on or not, or what state the OS may be in.
- **Server chassis:** Looks for blade server chassis management modules (CMMs). The blades in the server chassis are detected as normal servers.
- **Intel* AMT:** Looks for Intel Active Management Technology-enabled devices. AMT devices appear in the **Intel AMT** folder.
- **Starting IP:** Enter the starting IP address for the range of addresses you want to scan.
- **Ending IP:** Enter the ending IP address for the range of addresses you want to scan. UDD automatically updates this field as you type the **Starting IP**, but you can change the ending IP address manually. **Ending IP** is calculated using the value of **Subnet mask** + what is typed in **Starting IP**.
- **Subnet mask:** Enter the subnet mask for the IP address range you're scanning.
- **Add and Remove:** Adds or removes your IP address ranges from the work queue at the bottom of the dialog.
- **Schedule task:** Schedules the scan based on your settings. You can customize the start time in the **Scheduled tasks** window. Scheduled scans originate from the core server.
- **Scan now:** Starts the scan immediately based on your settings. Scans started here originate from the console you're at. Once you start the scan, a **Scan status** dialog appears showing the total number of devices found, how many existing devices were updated, and how many new unmanaged devices were added.

About the NT domain configuration dialog

Use this dialog to configure how you connect to the domain you want to scan.

- **Domain:** Enter the domain you want to scan.
- **Logon as current user:** Select this if you're logged in as a user with access to the domain you're scanning.
- **Logon as:** Select this if you aren't logged in as a user with access to the domain you're scanning. Also enter a **User name** and a **Password**.
- **Add and Remove:** Add each domain you configure and want to scan to the work queue by clicking **Add**. Click **Remove** to delete the selected domain from the work queue.

About the LDAP configuration dialog

Use this dialog to configure how you connect to the LDAP directory you want to scan.

- **LDAP://:** Enter the LDAP directory you want to scan.
- **Logon as current user:** Select this if you're logged in as a user with access to the directory you're scanning.
- **Logon as:** Select this if you aren't logged on as a user with access to the directory you're scanning. Also enter a **User name** and a **Password**.
- **Select individual OUs:** Select the OUs that you want to scan. Click **Add** to add them to the work queue. Click **Remove** to delete the selected OU from the queue.
- **Active directory path:** Shows the active directory path, if applicable.

Scheduled tasks help

About the Schedule task dialog

Access this dialog from the **Scheduled tasks** window (**Tools | Distribution | Scheduled tasks**). In the **Scheduled tasks** window, click the **Create software distribution task** toolbar button, or from the shortcut menu of the task you want to configure, click **Properties**.

Use this dialog to set the start time for the task and whether to make it a recurring task and how often. This dialog also shows the task targets. Depending on the task type you're scheduling, you may also see options for delivery methods and distribution packages.

About the Overview page

This page summarizes the choices you've made in the Scheduled tasks dialog. If you want to modify any of your choices, click **Change** beside that choice.

About the Distribution package page

Use this page to select the distribution package you want to deliver. Once you select a **Package type**, the **Distribution package** list shows the packages of that type that you can distribute. The packages in the list correspond to the packages you can see under that type in the **Distribution packages** window for the current user and the public user. Click the **Distribution package** you want.

About the Delivery methods page

Use this page to select the delivery method to use for the package you're delivering. Once you select a **Delivery type**, the **Delivery methods** list shows the delivery methods of that type that you can use. The delivery methods in the list correspond to the delivery methods you can see in the **Delivery methods** window for the current user and the public user. Click the **Delivery method** you want.

About the Target devices page

Use this page to view target devices for the task you're configuring. You can't add targets on this page. You can add targets later by dragging and dropping them into the task in the **Scheduled tasks** window. Targeted devices can be in these categories:

- Targeted devices
- Targeted LDAP objects
- Targeted queries
- Targeted LDAP queries
- Targeted device groups

You can also select the **Wake up devices** option on this page. This option wakes up a powered-down computer for the selected task by using Wake On LAN. When the task is complete, the computer shuts itself down again. This feature only works on computers with BIOS versions that support Wake on LAN technology. Selecting this option will make tasks take longer, since the task waits for devices that just woke up to boot. Don't mark this option for pull distribution packages.

About the Schedule task page

Use this page to configure when the task runs and how retries should work:

- **Start now:** Starts the task as soon as the dialog is closed. There can be a delay of up to a minute before the task actually starts.
- **Start later:** Starts the task at the specified time and date.
- **Time:** Starts a task at the selected time. By default, this field displays the current time.
- **Date and time:** Runs a task on selected date. Type the date using MM/DD/YY format, or click the drop-down list to pick the date off a calendar.
- **Repeat every:** Schedules the task to recur periodically. Select Day, Week, or Month from the drop-down list to choose how often the task repeats. It repeats at the time set above.
- **Schedule these devices:** For the first time a task runs, you should leave the default of **Schedule these devices**. For subsequent runs, choose from **All**, **Devices that did not succeed**, or **Devices that did not try to run the task**. These options are explained in more detail below.
- **Number of retries:** Retries the task automatically for the selected number of times (if the task fails to complete). Enter a value or use the spinner.

When rescheduling a task, you can limit the devices the task runs on. You may want to do this if the task failed on a large number of devices and you don't expect the failed device state to change, for example. Limiting the task this way would help the task complete more quickly because the scheduler wouldn't keep trying devices that won't process the task. You can choose to run tasks on devices in these states:

- **Waiting or currently working:** This is the default and should be used the first time a task runs. If you're rerunning the task, this option targets devices that succeeded the previous time you ran the task.
- **All:** Select this if you want the task to run on all devices, regardless of state. Consider using this option if you have a task, especially a repeating one, that needs to run on as many devices as possible.
- **Devices that didn't succeed:** Select this if you only want the task to run on all devices that didn't complete the task the first time. This excludes devices that have a **Successful** state. The task will run on devices in all other states, including **Waiting** or **Active**. Consider using this option if you need the task to run on as many unsuccessful devices as possible, but you only need the task to complete successfully once per device.
- **Devices that didn't try to run the task:** Select this if you only want the task to run on devices that didn't complete the task and didn't fail the task. This excludes devices that were in an **Off**, **Busy**, **Failed**, or **Canceled** state. Consider using this option if there were a lot of target devices that failed the task that aren't important as targets.

About the Local scheduler command dialog

You can use the local scheduler to schedule your own tasks to run periodically on devices. Once you create a local scheduler script, you can deploy it to devices by using the **Scheduled tasks** window. To configure a local scheduler task, in the **Managed scripts** window (**Tools | Distribution | Managed scripts**), from the My scripts shortcut menu, click **New local scheduler script**.

These options are available in the **Local scheduler command** dialog:

- **Command:** Enter the program you want to run locally. Include the full path to the program or make sure the program is in a folder that's in the device's path. This path must be the same on all devices you deploy this script to.
- **Parameters:** Enter any command-line parameters you want passed to the program.
- **Frequency:** If you want the task to recur, select the repeat interval.
- **IP address changed:** Check this option if you want the task to run only if the device's IP address changes. Use this option to trigger an inventory scan when the IP address changes, keeping the IP address in the Management Suite database synchronized.
- **User is logged on:** Check this option to run the task only when the user is logged on.
- **Bandwidth:** Check this option to specify the minimum network bandwidth for the task to run (either RAS, WAN, or LAN). You also need to specify the computer that will be the target for the bandwidth test between the target and device.
- **Start time:** Check this option to specify a date and time after which the task will be active. If you don't specify any other options, the task will run once at the start time you specify.
- **Hour of day:** Check this option to specify a time range for the task to run.
- **Day of week:** Check this option to specify a day-of-the-week range for the task to run.
- **Day of month:** Check this option to specify a day-of-the-month range for the task to run.

Using the Distribution package dialog

The **Distribution package** dialog (**Tools | Distribution | Distribution package**) stores information in the database that describes the package that you want to distribute. The data contains the settings necessary to install a specific software package, such as the package name, any dependencies or prerequisites, installation options, and so on. Once created, this information is called a "distribution package."

Before using this dialog, put the package on your distribution server. You'll need to browse for the package and provide information on any package prerequisites or additional files. Once you've created a distribution package for your package, you can associate it with a delivery method (**Tools | Distribution | Delivery methods**) to deploy it to devices.

About the Package information page

Use this page to enter the package name and your package's primary file. If your package consists of a single file, add it here. If your package has multiple files, add the main file in your package, for example, the file that starts the install. You can add supporting additional files on the **Additional files** page.

To use the file browser, type a Web share or file path in the box next to the **Go** button. Clicking **Go** displays the destination in the **Primary file** box. You can continue navigating there. When browsing for the file, double-click the file you want to be the primary file. This adds the filename to the package path next to the Go button.

- **Name:** The name you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer descriptions.
- **Package owner:** You can select **Public** if you want all console users to see this package, otherwise, you can select your own username so that only you can see it. Administrators can select a specific user, in addition to **Public**.
- **Description:** The description you enter here appears in the **Distribution packages** and **Delivery methods** dialogs.
- **Primary file:** The main file in this package.
- **Go:** Starts browsing the path you entered next to the Go button.
- **Up:** Goes up one folder level from the current location you're browsing.

Using environment variables

Support for putting the environment variable directly into the package path isn't supported in Management Suite, though expansion will still work with previously created custom scripts. To support environment variables for the new SWD architecture, the "PreferredPackageServer" registry value should be set to the environment variable to be used. This environment variable will then be expanded to define the server from which the package should be retrieved.

About the Install/Uninstall options page

Use this page to specify the package type. You have several options depending on the package you're deploying. Not all package types have these options.

- **Install:** Specifies that you want to use an installation package to install software.

- **Uninstall:** Specifies that you want to use an installation package to remove software. When this flag is set, the script removes everything that was installed with the installation script.
- **Command line:** (Not available for SWD, Macintosh, or Linux packages). The command line you want passed to the primary file you specified. Software distribution automatically adds the basic parameters for the type of package you're distributing. For more information, see Using package command lines.

The command line field also allows you to pass values from the device's database entry to the command line. You can use this to pass unique parameters to batch files and executables that you distribute. The command line field can contain a parameter such as %Computer.Device Name% that will call up the computer device name from the database for each targeted device and pass that parameter as part of the execution process. The parameters must be in BNF format and delimited by percent symbols. Examples of valid BNFs are as follows:

- %Computer.Display Name% : The network display name of the computer.
- %Computer.Network.TCPIP.Address% : The IP address of the computer.
- %Computer.OS.Name% : The operating system name of the computer.

You can see the BNF values for database attributes in the create query dialog.

Using package command lines

When creating a Distribution Package, there is an option to include a command line. In the case of an MSI package, this field can only be used to specify a list of MSI Properties in this format: property1=value1 property2=value2 property3=value, and so on. One example of an MSI Property is TRANSFORMS.

The command line switches that are documented in MSI-related documentation, such as /q, /f, and so on, are actually msixec command line switches. Only msixec understands them. When LANDesk distributes an MSI package, it calls the MSI APIs directly. It does not use msixec. Therefore, it isn't possible to specify msixec command line switches in the command line field.

For many of the options that would be enabled with a command line switch when using msixec, equivalent functionality is provided in through the delivery methods and distribution package tools. For others, no equivalent functionality is provided because it isn't needed.

Below is a list of some msixec command-line switches and how equivalent functionality is provided (or not) in the LANDesk interface:

- **/q:** to control the user feedback options during an installation, use the **Feedback** options in the distribution package tool.
- **/a:** Administrative installation would be meaningless under LANDesk. It needs to be performed manually by the administrator. Therefore, no equivalent functionality is provided in LANDesk.
- **/f:** reinstall an MSI package. LANDesk will always reinstall the primary packages, so this option is implied. Note: If you don't want to reinstall, simply deploy the msi application as a dependent package instead of the primary package. If you don't have another package to make primary, you can create a package to deploy an empty batch file and make the MSI a dependent package. Then detection will take affect for the MSI application and it will only be installed on devices that it isn't already installed on.)
- **/x:** uninstall an MSI package. Equivalent functionality is provided by the uninstall option in the distribution package tool.
- **/j:** advertise an MSI package. LANDesk implements similar concepts through policy-based delivery and the local device software distribution portal.

- **/l:** logging. Sdclient.exe gathers status and creates log files on the device by default.
- **/p:** install a patch; used to patch administrative images. Equivalent functionality is provided under LANDesk through Patch Manager and also with software distribution and dependent packages. Note: Deploy the latest patch as the primary package and set up a dependency chain for the MSI application and/or other patches.

About the Additional files page

If your package consists of multiple files, you can add them on this page. To use the file browser, type a Web share or file path in the box next to the Go button. Pressing the Go button displays the destination in the **Available** files box. You can continue navigating there. Select files in the **Available files** box and click >> to add them to the **Additional files** list. This adds them to the package.

- **Add additional files...:** The additional files you want to be part of your package.
- **Auto detect:** This option is available for MSI packages. It parses the primary MSI file for external file references and adds those automatically.
- **Arrows:** These arrows add and remove selected files from the **Additional files** list.
- **Go:** Starts browsing the path you entered next to the Go button.
- **Up:** Goes up one folder level from the current location you're browsing.

Using the Dependent packages page

Dependent packages are packages that must already be on the device in order for the package you're configuring to install. If they're not on the device, dependent packages are installed automatically. MSI and SWD packages are detected automatically through the appropriate registry keys on the device. For other package types, the package detection method depends on what you select on the detection page.

If you add an existing package with a dependency as a dependant package to the package you're creating, that existing dependency will also be added to the new package.

- **Available packages:** Lists the public packages you have created using the **Distribution package** window. Only public packages can be dependent. Select the packages you want to be dependent and click >>.
- **Dependent packages:** Lists the packages you've selected to be dependent.
- **Arrows:** These arrows add and remove selected files from the **Additional files** list.

Using the Prerequisites page

The prerequisites page allows you to specify prerequisites for package installation. You can do this through a query or through an additional file/program that runs on devices and returns an errorlevel code. A non-zero code prevents the package from installing.

Prerequisites run on devices in the target list. If a device on the target list fails a prerequisite, the package won't be installed on it. The failure details are in the distribution task's log.

Prerequisites are especially useful in organizations where one person creates packages and another person distributes them. The distributor might not be aware of package system requirements that the creator does know about. In cases like these, the package creator can create a query that includes package requirements like operating system or amount of memory.

For the additional file option, you can select a file that's in the package's additional files list. You can then specify a command line you want the file to run with.

- **Choose a query:** Select an existing query that you want to use to filter targeted devices.
- **Run additional file:** If you want to run a file on devices, check this option.
- **Choose an additional file:** Enter the file you want devices to run. This file is run before any other package files.
- **Command line:** If the file you specified needs a command line, enter it here.

Using the Detection page

Use this page to detect dependent packages or applications that weren't installed through Management Suite. A match on one or more criteria prevents dependent packages from installing. This page doesn't affect the primary package. You can use these detection methods:

- File exists
- File version
- File size and/or checksum
- File date
- Registry key exists
- Registry value exists
- Matching registry value

You can add multiple criteria. When you select a criteria from the list, the options for that criteria appear below the list. Enter the necessary information and click **Add**. Repeat as necessary.

Using the SWD package options page

Use this page to set what happens when an SWD package is already installed on a device. If you have applications that aren't responding to a normal package heal, the full reinstall option might work better. Healing tends to take less time than a full reinstall.

When you create an SWD package, you can create it with or without a package installation interface that users see. If the package has an interface, you can choose whether the package installation status dialog appears on top of their existing applications or whether there should be a solid blue installation background that masks the desktop while the package is installing.

- **Heal (repair) the package:** This option only updates registry keys and replaces program files that the agent detects as different than those in the installation package.
- **Perform a full reinstall of the package:** This option completely reinstalls the package, replacing all files and recreating all registry keys.
- **When feedback is enabled, override the above setting and let the user decide:** Allows users to choose between heal or reinstall. You can enable feedback in the **Delivery method properties** dialog's **Feedback** page.
- **When feedback is enabled, display the background screen:** Displays the solid blue background screen. You can enable feedback in the **Delivery method properties** dialog's **Feedback** page.

Using the Delivery methods dialog

The **Delivery methods** dialog (**Tools | Distribution | Delivery methods**) defines how a package will be sent to devices. These options aren't associated with a specific distribution package. Options include Targeted Multicast and push or policy-based distributions. Don't create a delivery method every time you want to distribute a package. Ideally, create a template delivery method to reuse for distributions that use the same delivery method.

Before using this dialog, create the distribution package (**Tools | Distribution | Distribution packages**) that you want to deliver.

About the Description page

Use this page to describe the delivery method you're creating and to set the number of devices you want to distribute to simultaneously.

- **Name:** The name for your delivery method.
- **Owner:** You can select **Public** if you want all console users to see this delivery method, otherwise, you can select your own username so that only you can see it. Administrators can select a specific user, in addition to **Public**.
- **Description of delivery method:** The description you enter here appears in the **Distribution packages** and **Delivery methods** trees and dialogs. Make the name descriptive but not too long, since you'll have to scroll to see longer descriptions.
- **Number of computers for distribution:** Controls the maximum number of devices that can simultaneously receive the software distribution.

About the Bandwidth page

Use this page to control the network bandwidth that the package requires for deployment. You don't have to select any of these options if you want all selected devices to receive the package regardless of their bandwidth.

Bandwidth control is important for devices that have a slow WAN or a dialup connection. You usually won't want to deploy a multi-megabyte package to devices on slow links. Choose from the following options:

- **Require a non-RAS network connection:** This option enables the bandwidth requirement. Select one of the following:
 - **Allow any non-RAS network connection:** This option enables WAN and LAN devices to receive the package.
 - **Only allow a high-speed network connection:** This option enables only LAN devices to receive the package.
- **Limit remote downloads (per subnet) to one device at a time:** Use this to reduce the network bandwidth consumed on a subnet.
 - **Maximum percentage of bandwidth to use:** When you've selected limit remote downloads, you can further limit bandwidth by adjusting the maximum percentage of the target device's network bandwidth to use for the distribution.

If you're using PDS to detect network connection speed, high-speed and low-speed connections return the same information. For accurate detection of high-speed network connections, you need to use ICMP.

ICMP sends ICMP echo requests of varying sizes to the remote computer and uses the round trip time of these echo requests/responses to determine the approximate bandwidth. However, not all routers or computers support forwarding or responding to ICMP echo requests. ICMP also distinguishes between LAN (high speed) and WAN (slow, but not dialup) connections.

If your network isn't configured to allow ICMP echo requests, you can select PDS. If you're using PDS, the **Only allow a high-speed network connection** option won't give you accurate control.

About the Feedback page

Use this page to help determine how much the user sees during the installation or removal of the software. You have these options:

- **Hide all feedback from user:** This option hides the installation from the user as much as the software distribution package allows. If you created the software distribution package to be silent, this option ensures that it will be silent. If the software distribution package has been created with user-interaction, this option can't guarantee that all user-interaction will be eliminated.
- **Display progress to user:** This option enables you to choose one of the following:
 - **Allow user to cancel:** This option enables the user to cancel the action: either an installation or removal. Generally, for application policies, this isn't recommended.
 - **Display full package interface:** This option controls whether the package installs silently (disabled) or if it prompts the user for feedback when necessary (enabled).

About the Multicast page

Use Multicast to deploy files: Checking this option enables Targeted Multicast and the Targeted Multicast option pages.

About the Multicast domains page (under the Multicast page)

This page appears only when you've selected Multicast as the distribution type. Use this page to configure multicast options.

- **Use multicast domain discovery:** Use this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
- **Use multicast domain discovery and save results:** Use this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
- **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery and save the results.
- **Domain representatives wake up devices:** Use this option if you want computers that support Wake On LAN* technology to turn on so they can receive the multicast. You can use the Multicast Options dialog to configure how long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds.

- **Number of seconds to wait for Wake On LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

About domain discovery

Domain discovery is only necessary on networks with subnets that can see each other's multicast traffic. If your subnets don't see each other's traffic, you can save time by first saving the results of a domain discovery and then selecting **Use results of last multicast domain discovery** so Targeted Multicast doesn't do a domain discovery before each job.

If your network subnets do see each other's multicast traffic, you can help Targeted Multicast work faster by pre-discovering your domains with the `multicast_domain_discovery.ini` script included in the `ManagementSuite\Scripts` folder. This script doesn't do anything on target devices. Run this script from the **Scheduled tasks** window against a target list that spans your network. This will save the domain discovery results for future use. You may want to run this script periodically before large sets of multicast distributions.

If you selected **Use cached file** in **Configure | Services | Multicast**, Targeted Multicast will go through a discovery process even if you selected **Use results of last multicast domain discovery**. Targeted Multicast needs to do this to find out which potential multicast domain representatives have the file in their cache.

About the Multicast limits page (under the Multicast page)

Use this page to configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time. The default is 5.
- **Maximum number of devices that failed multicast to process simultaneously:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the scheduled task handler would process no more than 20 computers at a time that failed the multicast. The scheduled task handler will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the scheduled task handler won't perform the distribution portion of the task for any computer that failed multicast. The default is 240.
- **Number of days the files stay in the device's cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged. The default is 2.
- **Number of days the files stay in cache on multicast domain representatives:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged. The default is 14.

About the Packet timing page (under the Multicast page)

Use this page to configure job-specific Targeted Multicast parameters. The defaults in this dialog should be fine for most multicasts. Here are what the options do:

- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets. This value is only used when the representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN. The default is 1.
- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above. The default is 200.

About the Download page

Use this page to configure bandwidth throttling and packet delays.

- **Peer download (only install from cache or peer):** Only allow packages to download if they are in the local cache or on a peer in the same multicast domain. This option conserves network bandwidth, but for the package installation to be successful, the package must be in one of these two places.
- **Dynamic bandwidth throttling:** Specifies that the network traffic a device creates has priority over distribution traffic. If you select this option and leave the **Minimum available bandwidth percentage to use** at 0, once the device initiates network traffic, the distribution cuts back to about one packet per second until the traffic stops. This option forces a full download of the file into the device's cache, which also enables byte-level checkpoint restart, where downloads resume where they left off if interrupted. If you're reinstalling or repairing an SWD package or an MSI package, you may not want to use the **Dynamic bandwidth throttling** option because these package types normally only download the files they need.
- **Minimum available bandwidth percentage to use:** Specifies how much dynamic bandwidth throttling to apply. You can enter values of up to 50 percent of the total network bandwidth available to the device. For example, if there were one other application consuming network bandwidth on the device during a distribution and you set the bandwidth percentage to 50 percent, the distribution job would take 50 percent and the device application would take 50 percent. In practice, this percentage is variable because the operating system automatically allocates much of the network bandwidth depending on the number of applications needing bandwidth and their priority.
- **Delay between packets when downloading from a peer:** This option specifies the delay between packets for peers on the same subnet. You can use this delay to force distributions to be faster or slower. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.
- **Delay between packets when downloading from the source:** Specifies the delay between the package source and device destination. Increasing the delay between packets makes the distribution slower and uses less bandwidth. You can use this option with **Dynamic bandwidth throttling**, but if these options are used together the packet delay has more of an affect.

About the Reboot page

Use this page to configure whether the computer is rebooted after the software has been installed or removed. You have three options:

- **Never reboot:** Devices won't reboot after a package installation. If you select this setting and your package requires a reboot, devices may encounter errors running the application until they do reboot. If the package is an SWD package, this option overrules any settings in the package. If the package is a generic executable or an MSI package, the package setting may overrule this option.
- **Reboot only if needed:** Devices will reboot if the package requires it.
- **Always reboot:** Devices will reboot regardless of whether the package requires it or not.

About the Deployment timing page

Use this page to control when the package is deployed after arriving at the device. You don't have to select any of these options if you want the package to be deployed as soon as you have scheduled it.

If you want your devices to have some control, you have these options:

- **Delay installation/removal until next login:** This option delays the deployment until the next time any user logs in to the computer.
- **Allow end user to delay installation/removal:** This option enables the user to delay the task. You can customize this option by configuring the following:
- **Use custom message:** If you enable this option, you can specify a custom delay message.
- **Amount of time before install/uninstall starts automatically:** This option enables you to specify how long to wait for the user to enter a delay time. The default is to wait for 60 seconds. If the user fails to interact with the request for a delay time within this specified time, the deployment begins.

About the Type and frequency of policy page

This page appears for policy-based delivery types and affects how target devices act when they receive the policy:

- **Required:** The policy-based delivery agent automatically applies required policies without user intervention. You can configure required policies to run silently. Any UI that appears on the device while a required task is installing should be non-blocking; in other words, the application being installed shouldn't require user input.
- **Recommended:** Users have the choice of when to install recommended policies. Recommended policies are selected by default on the device UI.
- **Optional:** Users have the choice of when to install optional policies. Optional policies aren't selected by default on the device UI.

You can also configure how frequently a policy can run:

- **Run once:** Once a policy successfully runs on a device, the device won't run that policy again.
- **As desired:** Can be installed by users at any time.
- **Periodic:** When a recommended or optional policy is specified as being periodic, it will be removed from the UI when it's successfully processed and will be shown again in the UI after the specified interval has elapsed.

About the downgrade page

Use this page to configure the distribution behavior when either the target operating system or the target device agents don't support the delivery methods you've chosen. For example, if you have older Management Suite agents on devices, they may not support multicast or peer download.

OS downgrade options:

- **Downgrade functionality to level of operating system:** Allows jobs to continue, though all of the delivery method options you selected may not be active.
- **Fail if operating system cannot handle default functionality:** Job fails if the operating system doesn't support the delivery method options you selected.

Device downgrade options:

- **Downgrade functionality to level of agent:** Allows job to continue though all of the delivery method options you selected may not be active.
- **Fail if agent cannot handle default functionality:** Job fails if the agents don't support the delivery method options you selected.

About the discovery page

This page allows you to choose options for device discovery. Before the scheduled task handler can process a job, it needs to discover each device's current IP address. This tab allows you to configure how the service contacts devices.

Discovery options:

- **UDP:** Selecting UDP uses a Ping Discovery Service (PDS) ping via UDP. Most Management Suite device components depend on PDS, so your managed devices should have PDS on them. PDS is part of the standard LANDesk agent. This is the fastest discovery method and the default. With UDP, you can also select the UDP ping retries and timeout.
- **TCP:** Selecting TCP uses an HTTP connection to the device on port 9595. This discovery method has the benefit of being able to work through a firewall if you open port 9595, but it's subject to HTTP connection timeouts if devices aren't there. These timeouts can take 20 seconds or more. If a lot of target devices don't respond to the TCP connection, your job will take a while before it can start.
- **Both:** Selecting Both has the service attempt discovery with UDP first, then TCP, and lastly DNS/WINS if it's selected.
- **Number of retries:** How many discovery attempts to do.
- **Discovery timeout:** How long to wait for a response with each discovery attempt.
- **Timeout for subnet broadcasts:** How long to wait for a response to subnet broadcasts.
- **Disable subnet broadcast:** When selected, disables discovery via a subnet broadcast. When selected, this will result in a subnet directed broadcast being sent via UDP using PDS.
- **DNS/WINS:** When selected, disables a name service lookup for each device if the selected TCP/UDP discovery method fails.

About the Multicast software distribution status window

This window appears on the core when there's an active Targeted Multicast distribution happening. This window shows the following information:

- **Package URL or UNC address:** This is the location of the package you're currently attempting to distribute. This line will be updated with the current file that is being transferred.
- **Status:** A real-time report on how the distribution is proceeding or, if the distribution is complete, how well the job completed.
- **Multicast domains:** The field on top shows all of the subnets and the multicast domain representatives that are being used in the distribution. When you highlight each domain representative, the lower window displays all of the computers that are receiving their distribution from that domain representative.
Each computer in the lower window contains information on how the distribution completed on that computer. There are several information fields on the far right of each computer listed, including Packets Missed, Resend Requests, and Slowdown Requests. These fields do not contain any information until after the distribution is complete.
- **Packets missed:** Shows the number of packets that the device wasn't able to obtain from the subnet representative. If this number wasn't 0, then the distribution failed.
- **Resend requests:** Shows the number of times the device had to request that packets be resent from the subnet representative. This is a good way to gauge, for example, how busy the device was when dealing with other processes during the distribution.
- **Slowdown requests:** Shows the number of times the device had to ask the subnet representative to slow the packet stream. In this case, high numbers usually indicate that a computer is having some hardware problem that is slowing the distribution. If you have a large number of computers that have a high number of slowdown requests, you should check the Delay/Packet number on the subnet representative. There's often a correlation between the Delay/Packet number and the number of slowdown requests.

This window closes automatically after 10 seconds. If you'd like the window to remain open during the entire distribution, click **Keep dialog open** and the window will stay open until you close it manually. Keeping the dialog open will stop script execution, so make sure you close the dialog when you're done.

Distributing files with a file transfer script

If you just want to copy files to devices, you can use a file transfer script. You can transfer any type of file, including text files, to a directory you specify on the device. File transfer scripts support Targeted Multicast.

To distribute files

1. Click **Tools | Distribution | Manage scripts**.
2. In the **All other scripts** shortcut menu, click **Create file deployment script**.
3. Enter a **Script name** and **Destination directory**. Click **Next**.
4. Enter the Multicast Domain Options you want. Click **Next**.
5. Select the files you want to deploy by selecting a **Web path** or a **File share path**, entering the path, and adding the files you want to the list box. Click **Next**.
6. Read the **Finished** page summary and click **Finish**.

About the Create file deployment script page

Use the **File deployment script** wizard (**Manage Scripts window | All Other Scripts** shortcut menu **Create File | Deployment Script**) to deploy individual files of any type to a device directory you specify.

- **Script name:** Enter a descriptive name for the script you're creating.
- **Destination directory:** Enter the device directory you want the files placed in.

OS deployment and Profile migration wizard help

This chapter contains the following context-sensitive help topics for the OS deployment/Migration tasks wizard:

- Choose a task page
- Configure imaging task page
- Enter script information page
- Enter credentials for image and imaging tool shares page
- Choose image store and imaging tool location page
- Enter additional deployment commands page
- Configure Multicast options page
- Configure advanced Multicast options page
- Specify Sysprep file information page
- Configure multiprocessor information page
- Specify generic Sysprep options page
- Specify Sysprep network options page
- Assign naming convention for target computers page
- Enter LANDesk client install location information page
- Select a collection for this profile page
- About the Collection Manager dialog
- About the File Rule dialog
- About the Collection of Rules dialog
- About the User-Initiated Package dialog
- Enter credentials for profile storage page
- Enter DOS commands to execute on the client page

Help for the OS deployment/Migration tasks wizard

This chapter provides descriptions of the options and settings found on each page (and dialog) of the OS deployment/Migration tasks wizard. This wizard is used to create scripts that capture or deploy OS images, and capture or restore user profiles. Scripts can then be scheduled as tasks on target devices on your network. The wizard is accessed from either the Toolbar button or shortcut menus in the Manage Scripts window (**Tools | Distribution | Manage Scripts**).

You can also access this information by clicking the Help button on the corresponding wizard page itself.

For detailed step-by-step instructions on how to use the OS deployment/Migration tasks wizard, and what you need to know in order to plan and implement image deployment and migration jobs, see Using OS deployment and Using Profile migration.

Note: All pages of the OS deployment/Migration tasks wizard are described here. However, the pages you actually see when running the wizard depends on the type of imaging or migration task you selected on the first page of the wizard.

About the OS deployment/Migration tasks wizard: Choose a task page

Use this page to specify which type of OSD/profile migration script you want to create, based on the following tasks:

- **Capture image:** Creates a script that captures and stores an OS image from a device. Images can be captured using the built-in LANDesk imaging tool, or a third-party tool such as Ghost*, PowerQuest*, or another tool of your choice.
- **Capture profile:** Creates a script that captures and stores a device's unique user settings, application and desktop settings, and files. You can also use this option to access the Collection Manager dialog to create a User-initiated profile migration package that can be run locally at individual devices.
- **Deploy image:** Creates a script that deploys a previously captured OS image to target devices.
- **Deploy image (with profile capture and restore):** Creates a script that performs a comprehensive deployment and migration job (capturing profile data, deploying an OS image, and then restoring the profile).
- **Restore profile:** Creates a script that restores previously captured profile data (user settings, application and desktop settings, and files) to target devices.
- **Generic DOS tasks:** Creates a script that runs DOS commands (including application launches) on devices.

Related topics

- Creating imaging scripts with the OS deployment/Migration tasks wizard
- Creating migration scripts with the OS deployment/Migration tasks wizard
- OS deployment overview
- Profile migration overview

About the OS deployment/Migration tasks wizard: Configure imaging task page

Use this page to configure the following characteristics of an OS imaging task:

Note: Some of the options listed below may be disabled, depending on what type of task (capture or deploy) you selected on the first page of the wizard.

- **Use Multicast:** Uses existing multicast domain representatives on subnets of your network to deploy the OS image via the LANDesk Targeted Multicast technology. Multicasting enables you to transmit software packages to multiple devices at once, significantly reducing time and bandwidth requirements. Instead of sending a package across the wire for each device, only one transfer is made for each subnet.

Note: Before using multicasting, make sure the multicasting components are in place on the subnet you're distributing to. Multicasting requires LANDesk Management Suite 6.62 or later agents and a LANDesk Management Suite 6.62 or later multicast domain representative.

- **Image is Sysprepped:** Indicates that you used Microsoft Sysprep to configure the OS image to be deployed. Selecting this option allows you to specify Sysprep file information and deployment options later in the wizard.

- **Include profile migration:** Integrates both profile capture and restore processes as part of the image deployment job. Selecting this option allows you to specify profile migration options later in the wizard.
- **Choose network adapter to use if the driver autodetection fails:** Ensures that the image deployment job is successful to all target devices. We recommend that you enable this option, and then select a network adapter that is common to your systems. This is especially important if you're deploying to laptops. You should carefully choose a listed network adapter to ensure your job succeeds.

OS deployment uses a phased approach to network adapter detection:

- OS deployment first tries to detect the network adapter from the target device's operating system prior to imaging over it.
- If that fails, OSD will reboot the target device and try to detect the network adapter from DOS.
- If that fails, OSD uses the network adapter you specified in the Undetectable network adapters option on this page of the wizard.
- If the adapter you specify fails, you must go to the target device and manually reboot it. The device will reboot normally into its original OS.

Related topics

- Multicasting OS images
- OS image guidelines
- Creating imaging scripts with the OS deployment/Migration tasks wizard
- OS deployment overview
- Profile migration overview

About the OS deployment/Migration tasks wizard: Enter script information page

Use this page to identify the OS deployment or profile migration script. The text you enter here is used when the script displays in the Manage Scripts and Scheduled Tasks windows:

- **Script name:** Identifies the script with a unique name. If the name you enter is already being used, you'll be prompted to replace the existing script. You should enter a name that helps you quickly and easily identify the script by its function or by the intended target devices on your network.
- **Script description:** (Optional) Helps you remember the script with the text you type in here.

Note: If you add this script to the LANDesk PXE DOS Menu, the description you enter here will appear in the menu.

Related topics

- Creating imaging scripts with the OS deployment/Migration tasks wizard
- OS deployment overview
- Profile migration overview
- Configuring the LANDesk PXE DOS (Boot) Menu

About the OS deployment/Migration tasks wizard: Enter credentials for the image and imaging tool share(s) page

Use this page to provide authentication credentials for the network share, or shares, where the OS image and the imaging tool used to create the image are stored:

Note: You can enter only one set of credentials that will be used to access both shares, so the shares must have matching credentials. The credentials must belong to a local user account on the device hosting the share.

- **Username:** Identifies a user account with credentials required for the user to log on to the network share.
- **Password:** Provides the user's password.
- **Domain:** Provides the user's Active Directory domain.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Choose image store location and imaging tool page

Use this page to specify the image type you want to capture with this script, where the image will be stored, and where the imaging tool is located:

- **Image type:** Identifies the file type (format) of the image file captured by this script, selected from the list of imaging tools.
- **UNC path where the new image will be saved:** Locates the server and share where the image file will be stored. The image must be stored on a share accessible by devices. Note that the share name cannot include any spaces. You can enter just the device name in UNC format, then browse for the remainder of the path by clicking the browse button.

Note: During the imaging process, devices will map this UNC path to drive I:.

- **UNC path to imaging tool:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename. Note that the share name cannot include any spaces.

Note: During the imaging process, devices will map this UNC path to drive H:.

Related topics

- Creating imaging scripts with the OS deployment/Migration tasks wizard
- OS deployment overview
- Profile migration overview

About the OS deployment/Migration tasks wizard: Choose image to restore to targeted clients page

Use this page to specify the type of image you want to restore with this script, where the image is stored, and where the imaging tool is located:

- **Image type:** Identifies the file type (format) of the existing image file you want to deploy with this script, selected from the list of imaging tools.
- **UNC path to image file to restore:** Locates the server and share where the image file is stored, including the image filename. The image must be stored on a share accessible to devices.
- **UNC path to imaging tool:** Locates the server and share where the imaging tool (matching the image type selected above) is located, including the tool's executable filename.

Related topics

- Creating imaging scripts with the OS deployment/Migration tasks wizard
- OS deployment overview
- Profile migration overview

About the OS deployment/Migration tasks wizard: Enter additional deployment commands page

Use this page to customize the script by adding DOS commands, imaging tool command-line parameters, and 'RunOnce' commands:

Note: The RunOnce commands option displays only when you are creating an image deployment script, not when you are creating an image capture script.

- **Enter commands to run before the client is rebooted and imaged:** Lists DOS commands or Windows program executables. You can add commands in this text box, one per line, as if you were typing at a DOS command prompt. Commands are sent to devices one at a time.

Note: Once these commands complete, the OS will shut down and the device will reboot in its virtual boot partition.

- **Enter additional command-line parameters for the imaging tool:** Lists command-line parameters for the selected imaging tool. You can add parameters in this text box at the end of the default command line. Refer to your imaging tool documentation for available command-line parameters. If you're using the LANDesk imaging tool, for more information, see Using the LANDesk imaging tool for DOS.
- **Enter the RunOnce commands that will run after Sysprep setup runs on the client:** (This option only applies to image deployment scripts) Lists commands that launch application programs you want Windows to run the first time the device boots (after Sysprep finishes). You can add commands in this text box, one per line, as if you were typing at a DOS command prompt.

Note: These commands are added to the Windows RunOnce registry key:
 \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

- **Finish:** Saves the image deployment script and then exits the wizard.
- **Cancel:** Exits the wizard without saving the script.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Configure Multicast options page

Use this page to configure the following basic LANDesk Targeted Multicast options for an image deployment script:

- **Use Multicast domain discovery:** Searches for multicast domain representatives on subnets of your network prior to using Targeted Multicasting to deploy the image to devices across the network.
- **Use Multicast domain discovery and save results:** Searches for multicast domain representatives on subnets of your network prior to deploying the image, and saves the resulting data to help facilitate future Targeted Multicasting deployments.

Only one discovery's results are saved at a time, so selecting this option for an image deployment script will replace the results of the previous discovery.

- **Use results of last Multicast domain discovery:** Uses the most recent list of discovered multicast domain representatives when deploying the image to devices.

Note: Select this option ONLY if you've already saved the resulting data of a multicast domain representative discovery at least once.

- **Configure advanced Multicast options:** Allows you to further customize Targeted Multicasting behavior for a deployment script by configuring advanced Multicast options on the next page of the wizard.

Related topics

- Multicasting OS images
- OS deployment overview

About the OS deployment/Migration tasks wizard: Configure advanced Multicast options page

Use this page to configure the following advanced LANDesk Targeted Multicast options for an image deployment script:

- **Maximum number of Multicast Domain Representatives working simultaneously:** Controls the maximum number of multicast domain representatives that can actively deploy an image via Targeted Multicasting at the same time.
- **Number of days files stay in the client cache:** Controls the amount of time the image file being multicast can reside in the local cache on each target device. After this period of time, the file will be automatically purged.

- **Number of days files stay in the Multicast Domain Representative cache:** Controls the amount of time the image file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions:** Controls the minimum amount of time to wait between sending out multicast packets. This value is only used when the multicast domain representative is not multicasting a file from its own cache. You can use this parameter to limit bandwidth usage across the WAN.

Note: If this parameter is not specified, then the default minimum sleep time stored on the subnet's multicast domain representative will be used.

- **Maximum number of milliseconds between packet transmissions:** Controls the maximum amount of time to wait between sending out multicast packets.

Related topics

- Multicasting OS images
- OS deployment overview

About the OS deployment/Migration tasks wizard: Specify Sysprep file information page

Use this page to provide the following information about the Sysprep file (SYSPREP.INF) used by this script to modify the image being deployed:

- **SYSPREP.INF file source - Use existing SYSPREP.INF file as a template:** Uses an existing SYSPREP.INF file as a template for a new file and indicates where the existing file is stored. The new SYSPREP.INF file, containing the settings you specify in this wizard, overwrites the existing default Sysprep file. If you want OSD to base its SYSPREP.INF file on one you've already created, you can browse for that file. If you don't select an existing SYSPREP.INF, OSD creates a new one.

Note: After you finish the wizard, you can edit the SYSPREP.INF associated with a script by right-clicking that script and clicking **Advanced Edit**.

- **SYSPREP.INF location in the image being deployed:** Locates where the SYSPREP.INF file was stored on the hard drive of the device where Sysprep was originally run. In other words, the device whose image is being deployed by this script.
- **SYSPREP.INF multiprocessor image support - Configure advanced multiprocessor options:** Allows you to configure an image to support multiprocessors (on Windows 2000 or Windows XP devices) on the next page of the wizard.

Note: Only select this option if the processor count within your image is different than the processor count on any of your target devices.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Configure multiprocessor information page

Use this page to configure the following multiprocessor settings for the image being deployed by this script:

- **Enter the Operating System type for the image being deployed:** Specifies the OS that is part of the image being deployed, either Windows 2000 or Windows XP.
- **On what type of computer was the image created:** Indicates whether the image being deployed was created on a uniprocessor or multiprocessor device, with either the APIC or MPS architecture.
- **Enter the location of the HAL-related .INF files inside your image:** Specifies the path to the HAL-related .INF file for the image being deployed by this script. By default, the wizard uses Microsoft's default .INF file paths for each OS. If you used the default paths when setting up your device for imaging, leave the information in this text box as is. Otherwise, type in the different path you used to the HAL-related .INF file.

Additional multiprocessor information

Uniprocessor and multiprocessor devices require different Windows 2000 and Windows XP kernels. Depending on your hardware configuration, you may be able to use your uniprocessor image on a multiprocessor device, or vice versa.

Devices that support advanced processor features typically have an Advanced Programmable Interrupt Controller (APIC). Devices that support advanced processor features can also have an Advanced Configuration and Power Interface (ACPI).

The support matrix for sharing an image between uniprocessor and multiprocessor devices is complex. You should refer to Microsoft's Sysprep documentation for more details.

WARNING: As a general rule when considering sharing uniprocessor and multiprocessor images, remember that both the source and target devices must have either an ACPI APIC HAL or a non-ACPI APIC HAL. You can't use an ACPI APIC image on a non-ACPI APIC device, or vice versa.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Specify generic Sysprep options page

Use this page to specify the following generic settings for the SYSPREP.INF file used by this script to modify the image being deployed:

- **Time zone:** Indicates the time zone where the target devices are located.
- **Volume license key:** Specifies the license number for the OS that is being deployed.
- **Local administrator password for this image:** Provides the administrator's password for the device that was imaged.
- **Name:** Identifies the target devices with a name, such as a department name or geographic location.
- **Organization:** Identifies your organization with a name, such as a division or company name.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Specify Sysprep network options page

Use this page to specify the following network settings you want to include in the SYSPREP.INF file for this image:

- **Workgroup:** Indicates that your target devices reside in a workgroup. If you select this option, enter the name of the workgroup in the text box.
- **Domain:** Indicates that your target devices reside in a domain. If you select this option, enter the name of the domain in the text box and provide the following domain account information:
 - **Username:** Identifies the name of a user in the domain that has privileges to add a machine account to the domain.
 - **Password:** Provides the user's password.
 - **Add machine to OU:** Specifies the path (using LDAP path syntax) to a specific Microsoft Active Directory OU where you want to add the target devices being imaged.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Assign naming convention for target computers page

Use this page to assign the naming convention for target devices that will be imaged by the image deployment script:

- **First attempt to get and use existing computer names from the Inventory database:** Preserves existing Windows computer names if the targeted devices have already had the inventory scanner run on them. The image will attempt to use any computer names that already exist in the core database.
- **When necessary, use the following template to name target computers:** Provides a template that defines a naming convention to create unique names for target devices that do not currently have a device name assigned to them in the core database. This template is useful for LANDesk agent-discovered and PXE-booted devices. You can review the examples on the wizard page.

Related topics

- Creating custom computer names
- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Enter LANDesk client install location information page

Use this page to provide the following information needed by the image to install LANDesk device software onto target devices:

- **UNC path to directory containing WSCFG32.EXE:** Specifies the UNC path (usually \\<corename>\LDLogon) to the core server or service center where WSCFG32.EXE (the LANDesk device setup file) resides.
- **Authentication credentials:** Provides a username, password, and domain to authenticate to the core server or service center, so that the image can install WSCFG32.EXE onto target devices.

Related topics

- OS image guidelines
- OS deployment overview

About the OS deployment/Migration tasks wizard: Select a collection for this profile page

Use this page to select a collection of rules for the profile migration script and to access the Collection Manager dialog. A collection determines the profile content to be migrated (captured or restored) by the migration script:

- **Available collections:** Lists all of the available collections on your core server. A collection is a user-defined set of rules, each rule identifying a specific application, desktop setting, or file that can be migrated. When you highlight a collection in the list, a description of that collection appears in the message box below.

Note: You can select only one collection for each migration script. However, you can create and modify as many collections as you like, using different combinations of application, desktop, and file rules.

- **Manage:** Accesses the Collection Manager dialog, where you can create and edit collections and file rules and create user-initiated migration packages.

Related topics

- Profile migration overview
- Profile content
- About the Collection Manager dialog

About the Collection Manager dialog

Use this dialog to create, edit, or delete collections of rules, as well as specific file rules. You can also use this dialog to create or delete user-initiated profile migration packages:

(You can access the Collection Manager dialog from either the OS deployment/Migration tasks script wizard, or directly from the Manage Scripts toolbar in the console.)

- **File rules:** Displays all available file rules in the list box. You can create a new file rule or edit an existing one.

Note: When you delete a file rule, the rule is removed from the core server. Any collection that contained that rule provides a notice about this change the next time you open or edit the collection.

- **Collections:** Displays all available collections in the list box. You can create a new collection or edit an existing one.

Note: When you delete a collection, the collection is removed from the core server. Any migration script referencing that collection will not run properly. You should also delete the script.

- **User-Initiated packages:** Displays all available packages in the list box. You can create a new migration package, which is a self-extracting executable file that can be run on individual devices. You can't edit an existing user-initiated package.

Note: When you delete a user-initiated package, the package is removed from the core server. Other copies of the package may still exist depending on how and where you distributed the package to users.

Related topics

- Creating file rules
- Creating collections
- Creating user-initiated migration packages
- Profile migration overview
- Profile content

About the File Rule dialog

Use this dialog to create new file rules or edit existing ones (in the Collection Manager dialog, click **File rules** and then click **New**).

A file rule determines which files are migrated, based on the following criteria: drive and directory location, subdirectories, file naming (including wildcard support), and destination location.

- **Rule name:** Identifies the file rule with a unique name. If you enter the name of an existing file rule, you'll be asked whether you want to replace it. Use a name that will help you identify the purpose or content of the file rule.
- **Rule description:** (Optional) Helps you remember the file rule.
- **Source directory:** Specifies the drive and directory path to the location of the files you want to migrate.

Note on disk partitions: You can migrate files from a device's fixed drives, including disk partitions. Removable media, such as CD-ROM drives, and network shares are not supported. If the target device does not have a matching disk partition drive letter, a new directory named "Migrated_[drive letter]_Drive" is created at the root of the target device's C drive, and the files (along with their associated directory structure) are migrated to that new directory on the target device.

- **Include subdirectories:** Searches for files in all subdirectories of the specified source directory.
- **Remap destination directory:** Moves files to a path on the target device that is different than the source directory path. A file's associated directory structure will still be preserved under the remapped path.
- **Destination directory:** Specifies the drive and directory path on the target device where you want to migrate files that match the location and naming criteria.
- **Files to include:** Captures files in the specified source directory that match the filename syntax you enter here. You can use exact filenames to limit the inclusion to an individual file. You can also use wildcard naming syntax (* and ?) to include files by file type/extension (i.e., *.txt), prefix (i.e., myname*.*), or any other valid wildcard usage.

Note: Separate multiple filenames with a semi-colon character (;).

- **Files to exclude:** Does not capture files in the specified source directory that match the filename syntax you enter here. You can use exact filenames to limit the exclusion to an individual file. You can also use wildcard naming syntax (* and ?) to exclude files by file type/extension (i.e., *.txt), prefixes (i.e., myname*.*), or any other valid wildcard usage.

Note: If the include control and the exclude control contradict each other, the exclude control takes precedence and the file(s) will not be captured by the file rule.

Related topics

- Migrating files and folders
- Profile content
- Profile migration overview

About the Collection of Rules dialog

Use this dialog to create new collections and edit existing ones (in the Collection Manager dialog, click **Collections** and then click **New**).

A collection is a user-defined set of application, desktop and file rules, that determines the profile content to be migrated.

- **Collection name:** Identifies the collection with a unique name. If you enter the name of an existing collection, you'll be asked whether you want to replace it. Use a name that will help you identify the purpose or content of the collection.
- **Description:** (Optional) Helps you remember the collection. The description you enter here will display in both the Collection Manager dialog and the Selecting a collection page of the wizard to help you identify the collection.
- **Rules:** Indicates the profile content you want migrated by this collection. Use the plus-sign and minus-sign boxes to expand and collapse the tree structure to view all of the Applications, Desktop Settings, and File Rules. You can select any combination of the rules available in the Rules tree listing when defining a collection.

Related topics

- Profile content
- Profile migration overview

About the User-Initiated Package dialog

Use this dialog to create a self-extracting executable file that can be run on devices as a user-initiated profile migration (in the Collection Manager dialog, click **User-initiated packages** and then click **New**).

Note: User-initiated migration packages can be run on LANDesk-managed devices, as well as computers that are not managed by the LANDesk agents.

- **Package name:** Identifies the user-initiated profile migration package with a unique name. If you enter the name of an existing profile migration package, you'll be asked whether you want to replace it. Use a name that will help you identify the purpose or content of the user-initiated package.

Note: Do not type the filename extension here; the .EXE extension will be appended automatically to the name you enter.

- **Rule collection:** Lists all of the of available rule collections. The collection you select determines the content of the user-initiated profile migration. You can select only one collection per migration package.

Note: The user-initiated migration package (*.EXE) is saved by default to the following directory on your core server:
c:\Program Files\LANDesk\ManagementSuite\LDLogon\PMScripts\Executables

Related topics

- Creating user-initiated profile migration packages
- Running user-initiated profile migration packages
- Creating a collection
- Profile migration overview
- Profile content

About the OS deployment/Migration tasks wizard: Enter credentials for profile storage page

Use this page to specify where to store the profile data and to provide authentication credentials:

- **UNC path to profile storage directory:** Specifies the UNC path to where the profile data will be stored. You can enter just the computer name in UNC format, then browse for the remainder of the path by clicking the Browse button.
- **User name:** Identifies a user with valid authentication credentials to the specified UNC path.
- **Password:** Provides the user's password.
- **Domain:** Provides the user's domain.
- **Force authentication using these credentials:** Forces an authentication (log out and log in) using the credentials specified above on devices that are scheduled for a profile migration IF the currently logged in user's credentials fail. If such a failure occurs, checking this option ensures that the device has sufficient rights to access and save data on the network share where the profile data will be stored.

- **Default local user account(s) password:** (Only available for a profile restore script)
Provides a password that will become the common default password for all of the *new* migrated local user accounts created on the target device. If a user account already exists, settings are migrated, but the current password is preserved and should be used to log in.

Note: If you leave this text box empty, the password is automatically set to the default: password.

- **Finish:** Saves the profile migration script and exits the wizard.
- **Cancel:** Exits the wizard without saving the script.

Related topics

- [Profile migration overview](#)

About the OS deployment/Migration tasks wizard: Enter DOS commands to execute on the client page

Use this page to create a script that runs DOS commands (including application executable names) on target devices. The commands are sent to devices one at a time.

- **DOS command text box:** DOS commands can be added to this box, one per line, as if you were typing at a DOS command prompt. You can enter as many commands as you like.
- **Abort this job if any command fails:** Causes the imaging job to abort if any of the DOS commands entered on this page fail. Applications (launched from the DOS command line) that generate a DOS errorlevel code when failing will also cause the imaging job to abort. If no errorlevel code is created when a command or application fails, the imaging job will continue.
- **Finish:** Saves the DOS commands script and then exits the wizard.
- **Cancel:** Exits the wizard without saving the script.

Related topics

- [Creating imaging scripts with the OS deployment/Migration tasks wizard](#)
- [OS deployment overview](#)
- [Profile migration overview](#)

Software license monitoring help

About the Alias properties dialog

Use this dialog (from the **Aliases** tree item's shortcut menu, click **Create alias**) to create an alias for a product executable. Aliasing ensures that the scanner can correctly identify device applications if their product or vendor names have changed since being installed.

If name changes occur to your device's software, use aliasing to associate new vendor or product names with the originals. The scanner will then associate the new names with any executables that match the original information in the core server's core database, ensuring that your software is accurately identified.

This feature is most useful when monitoring product licenses in the Compliance view, ensuring that the scanner can continue to identify those products.

- **Original vendor:** Enter the name of the product's original vendor.
- **Original product name:** Enter the original product name.
- **New vendor:** Enter the new vendor name.
- **New product name:** Enter the product's new name.

About the Product properties dialog

Use this dialog (from a product's shortcut menu, click **Properties**) to view and change the following:

- Products
- Files
- Downgrades

About the Product properties dialog's Product tab

Use this dialog (right-click a product and click **Properties** and then the **Product** tab) to view and change the properties with the product.

- **Product name:** Shows the name of the product you're viewing.
- **Version:** Shows the product version number.
- **Publisher:** Shows the vendor that created the product.
- **Deny use of this product:** Whether SLM is denying execution for this product on devices.

About the Product properties dialog's Files tab

Use this dialog (right-click a product and click **Properties** and then the **File** tab) to view and change the files associated with the product.

- **Vendor, Product name, File name, Version, and Size:** Information about the files that are part of this product. If you enter file size of 1, any file with that file name matches.
- **Add:** Opens the Add files to product window, where you can select from files to add.
- **Create:** Creates a new definition for a file that you can add to the product.

- **Match all files:** Whether multiple files must be on the device before a license is counted as used.

About the Product properties dialog's Downgrades tab

Use this dialog (right-click a product and click **Properties** and then the **Downgrades** tab) to view and change the downgrades for the product.

Software license monitoring window lets you "downgrade" licenses for certain products: if you have two versions of the same product installed on your network, you can set up the older version to borrow a license from the newer version.

The Downgrades tab is divided into two halves:

- The top half, **Downgrade licensed products**, lists the products you want to be able to borrow licenses from the current product.
- The bottom half, **Upgrade licensed products**, lists products that this product can borrow licenses from.

Use these buttons to configure downgraded licenses:

- **Add button:** Click this to specify which products can borrow licenses from the product you're configuring.
- **Remove button:** Click this to remove a product from the list.
- **Move up/down buttons:** Select a downgrade licensed product and click **Move up** or **Move down** to prioritize which product will receive the borrowed licenses.

You can't configure the amount of licenses that are borrowed or loaned in this tab. Configure licenses within a product's **Product licenses** dialog.

About the Add files to product window

Use this window (click the **Files** item from a product's shortcut menu, then click **Add** in the **Files** tab) to specify which files should be monitored to determine when a product is running.

- **Find:** Enter the filename or search keyword you want to look for.
- **In column:** Select the inventory column you want to search in, either Vendor, Product Name, File Name, Version, or Size.
- **Discovered but not in product:** Shows files that also appear in the **To be dispositioned** list but aren't currently being monitored in the Compliance tree. Use this list to view files that you may want to begin monitoring for license compliance and usage/denial trends.
- **To be scanned:** Shows files in your core server's LDAPPL3 that the scanner can identify on devices.
- **To be dispositioned:** Shows files that have been discovered on devices, but are unknown to LDAPPL3. You must move these files into other categories before the scanner can identify them.
- **Discovered on computers:** Shows all files that have been discovered on devices, even if they're for products that aren't defined in the LDAPPL3.
- **In monitored product:** Shows files that are already being used to monitor products.
- **File information pane:** Shows files that match your Find string and the **File list** you've selected.

About the Product licenses dialog

Use this dialog, accessed from the **Manage licenses** item on a product's shortcut menu, to view and configure the license information associated with a product.

The dialog shows this information:

- **License number, Type, and Quantity:** Details on each license you've added for this product.
- **Licenses:** Total number of licenses available for this product.
- **Out of compliance:** How many installations are exceeding the amount of licenses available.
- **Loaned:** If another product can borrow licenses from this one, how many licenses this product is loaning.
- **Installations:** The number of installations detected for this product.
- **Not deployed:** The number of licenses remaining for this product.
- **Borrowed:** If this product can borrow licenses from another, the number of licenses this product is borrowing.

About the License properties dialog

Use this dialog, accessed from the Add button on the Product licenses dialog, to add or change license information.

The **License properties** dialog has three tabs:

- License
- Purchase Info
- Tracking

Use the **License** tab to configure license properties for your product.

- **License number:** Enter a number that constitutes your product license.
- **License type:** Enter a type of license you have for the product, such as: competitive upgrade, freeware, new purchase, OEM, product upgrade, public domain, shareware, unknown.
- **Quantity:** Enter the number of product licenses purchased.
- **Serial number:** Enter an additional number that may constitute your product license.

Use the **Purchase info** tab to configure purchase properties for your product license.

- **Purchase date:** Enter a date the product was purchased by your company.
- **Unit price:** Enter a price of each purchased license for the product.
- **Order number:** Enter an order number used to make the purchase.
- **Reseller:** Enter the name of purchase place.

Use the **Tracking** tab to configure tracking properties for your product license.

- **Owner:** Enter a person or department in your company responsible for storing the boxed product.
- **Location:** Enter a physical location where the boxed product is stored.

- **Note:** Enter any additional information associated with the product license, such as downgrade rights.

About the Group properties dialog

Use this dialog (from a product group's shortcut menu, click **Properties**) to view and change the following:

- Groups
- Scopes
- Devices

About the Group properties dialog's Group tab

Use the **Group** tab to edit a group's name.

About the Group properties dialog's Scopes tab

Use the **Scopes** tab to add a scope to a group. For more information on scopes, see "Using scopes with products."

The tab lists the scopes that currently apply to products under this group. To add a scope, click **Add** and click the scope you want. If you add a scope, make sure in the Scopes tab that you remove the **Default All Machines** scope. Deleting this allows the newly selected scope to be applied.

Click the **Refresh** toolbar button and verify the scope is working the way you want it to.

About the Group properties dialog's Devices tab

Use the **Devices** tab to see the devices that are part of the scopes defined for the group. Click **Resolve** to populate the list.

About the File Properties dialog

Use this dialog (click **Inventory | Files >** and the **To be scanned** or **To be dispositioned** category, then click the **New File** toolbar button) to add files to an LDAPPL3 category.

- **Browse button:** Use this button to directly select a file. Selecting a file this way fills in the Filename and Size fields for you.
- **Filename:** Browse for or enter a filename.
- **Size (in bytes):** Enter the file's size in bytes. Don't use commas or other separators between the digits. If you enter file size of 1, any file with that file name matches.
- **Product name:** Enter the product name the file belongs to.
- **Vendor:** Enter the vendor name for the product that uses the file.
- **Version:** Enter a version name for the file.
- **Action or state:** Select what you want done with the file:
 - **To be scanned:** Add the file to this category to have the inventory scanner look for it on devices.
 - **To be dispositioned:** Add the file to this category if you want to decide later what you want to do with the file.

- **Scan method:** Since you're editing LDAPPL3 file properties, you can't change the scan method.

About the Deny file dialog

Use this dialog (click **Inventory | Files**, and from the shortcut menu for **To be denied**, click **New file**) to add a file that you want to deny access to. You can only deny access by filename.

Handheld Manager help

Handheld Manager's file exchange feature lets you place files on Pocket PC handhelds or transfer files from Pocket PC handhelds to the core server.

About the Create handheld CABs dialog

The **Create handheld CABs** dialog has these options:

- **CAB name:** The filename for the cab you're creating. Don't include a path. CABs are saved in the core server's \Program Files\LANDesk\ManagementSuite\PocketPCCABS folder.
- **File to include in CAB:** The path and name of the file you're including in the .CAB.
- **File destination on the handheld:** Where to place the file on the handheld.
- **Add/Remove:** Once you've specified a .CAB name, file to include, and a file destination, click **Add** to add the file to the .CAB. You can add as many files as you want by entering the file information and clicking the **Add** button after each one.
- **Create:** Creates the .CAB based on the information you provided.

About the Handheld files to back up dialog

The **Handheld files to back up** dialog has these options:

- **Handheld path and file name to back up:** The full path and filename on the handheld that you want to back up. You don't need to include a drive letter. For example: \Program Files\landesk\test.doc.
- **Add/Remove:** Use these buttons to add or remove files you want to back up.
- **Delay between buffer writes:** How long the handheld waits after sending one buffer's worth of data. Use this to influence the amount of network bandwidth the backup consumes.
- **Write buffer size:** How much data to send before the buffer write delay occurs. Use this to influence the amount of network bandwidth the backup consumes.

Security and Patch Manager help

The Security and Patch Manager window (**Tools | Security | Security and Patch Manager**) is where you download and manage security and patch content, configure security tasks such as assessment scanning and remediation, customize and apply security scanner display/interaction settings, and view comprehensive security-related information for scanned devices, among other important tasks, all designed to help you protect your LANDesk managed devices from the many prevalent types of security risks that could harm your network.

The Using Security and Patch Manager chapter introduces this security management tool, which is an integral component of both the LANDesk Management Suite and LANDesk Security Suite products. In that chapter you'll find overview and security content subscription information, as well as step-by-step instructions on how to use all of the tool's features. Also included in that chapter is a section describing the interface and functionality of the Security and Patch Manager window.

This chapter contains the online help sections describing the Security and Patch Manager dialogs that are accessed by clicking a dialog Help button:

- About the Manage filters dialog
- About the Filter properties dialog
- About the Download updates dialog
- About the Definition properties dialog
- About the Download associated patches dialog
- About the Detection rule properties dialog
- About the Purge unused definitions dialog
- About the Create security scan task dialog
- About the Configure scan and repair settings dialog
- About the Scan and repair settings dialog
- About the Security and patch information dialog
- About the Schedule repair dialog
- About the Multicast options dialog
- About the Uninstall patch dialog
- About the Create reboot task dialog
- About the Configure firewall settings dialog

About the Manage filters dialog

Use this dialog to manage filters you can use to customize the security and patch content that displays in the Security and Patch Manager window's item list. You can use filters to streamline a lengthy list.

- **New:** Opens the Filter Properties dialog where you can configure a new filter's settings.
- **Edit:** Opens the Filter Properties dialog where you can modify and save the selected filter.
- **Delete:** Removes the selected filter from the database.
- **Use filter:** Applies the selected filter to the current item list. The applied filter persists when you click different groups in the tree view.

About the Filter properties dialog

Use this dialog to create or edit security content list filters. You can filter by operating system, security risk severity, or any combination of both.

- **Filter name:** Identifies the filter by a unique name. This name appears in the Filter drop-down list.
- **Filter operating systems:** Specifies the operating systems whose definitions you want to display in the item lists. Only those items associated with the operating systems you select are displayed.
- **Filter severities:** Specifies the severities whose definitions you want to display in the items lists. Only those items whose severity matches the ones you select are displayed.

About the Download updates dialog

Use this dialog to configure settings for downloading security and patch content updates, the patch file download location, proxy server settings, and alerting.

Security Suite content subscriptions

A basic LANDesk Management Suite installation allows you to download and scan for LANDesk software updates, and to create and use your own custom definitions. For all other security and patch content types, such as platform-specific vulnerabilities, spyware, etc., you must have a LANDesk Security Suite content subscription in order to download the corresponding definitions. For information about Security Suite content subscriptions, contact your LANDesk reseller, or visit the LANDesk Web site.

After you specify the types of content you want to download, and the other options on the Download updates dialog:

- To perform an immediate download, click **Update Now**. If you click **Apply**, the settings you specify will be saved and will appear the next time you open this dialog. If you click **Close**, you'll be prompted whether you want to save the settings.
- To schedule a download security and patch content task, click **Schedule update** to open the **Scheduled update information** dialog, enter a name for the task, verify the information for the task, and then click **OK** to add the task to Scheduled tasks. (Note that only the definition types, languages, and definition and patch download settings are saved and associated when you create a particular task. Download settings on the other tabs of this dialog, such as patch download location, proxy settings, and alerting settings, are global, meaning they apply to all the security content download tasks. However, you can change those settings at any time and they will be effective for all security content download tasks from that point on.)

To save your changes on any tab of this dialog, you can click **Apply** at any time. When you click **Close**, you're prompted whether you want to save changes.

The Update settings dialog contains the following tabs:

- About the Updates tab
- About the Patch location tab
- About the Proxy settings tab
- About the Alerting tab

About the Updates tab

- **Select update source site:** Specifies the LANDesk Security content server that is accessed to download the latest definitions, detection rules, and associated patches to your database. Select the server nearest your location.

- **Definition types:** Identifies which security and patch content definitions are updated. Only those definition types for which you have a subscription are available. The more definition types you select, the longer the download will take.
- **Languages:** Identifies the language versions of the selected definition types that are updated.

Some vulnerability and other definition types, and any associated patches, are language neutral or independent, meaning they are compatible with any language version of the OS or application addressed by that definition. In other words, you don't need a unique language-specific patch to remediate those vulnerabilities because the patch covers all supported languages. For example, Linux and UNIX platforms use only language neutral definitions and patches. However, Microsoft Windows and Apple Macintosh platform vulnerability definitions and patches are nearly always language specific.

When downloading content for any platform (with the appropriate subscription), all of the selected platform's language neutral vulnerability definitions are automatically updated by default. If you've selected a Windows or Mac content type, you must also select the specific languages whose definitions you want to update. If you've selected the Sun Solaris or a Linux platform, you do not have to select a specific language because their content is language neutral and will be updated automatically.

- **Put new definitions in the Unassigned group (unless marked for Alerting):** Automatically places new definitions and associated detection rules in the Unassigned group instead of in the default Scan group. Select this option if you want to be able to manually move content in and out of the Scan group in order to customize the security scan. (**Note:** Definitions that are selected to be placed in the Alert group (in the **Configure Alerts** dialog), are automatically placed in the Scan group even if this option is selected.)

Important: For the blocked application type, definitions are downloaded to the Unassigned group by default, not the Scan group. You don't have to select this option if you're downloading only blocked application definitions.

- **Download patches for definitions selected above:** Automatically downloads patch executable files to the specified download location (see Patch Location tab), according to one of the following download options:
 - **For detected definitions only:** Downloads only the patches associated with vulnerabilities, security threats, or LANDesk updates detected by the last security scan (i.e., the definitions that are currently residing in the Detected group).
 - **For all downloaded definitions:** Downloads ALL of the patches associated with vulnerabilities, security threats, and LANDesk software updates currently residing in the Scan group.

About the Patch location tab

- **UNC path where patches are stored:** Specifies where patch files are downloaded. The default location is the core server's \LDLogon\Patch folder. You can enter a different UNC path to download patches, but you must ensure access to that location by entering valid authentication credentials in the fields below.
- **Credentials to store patches:** Identifies a valid username and password for accessing a location other than the core server. If you're downloading patches to the default location on the core server, the username and password fields are not applicable.

- **Web URL where clients access patches:** Specifies a Web address where devices can access downloaded patches for deployment. The default location is the core server's \LDLogon\Patch folder. This location will normally be the same as the UNC path specified above.
- **Test settings:** Performs a connectivity test to the specified Web URL.
- **Reset to default:** Restores both the UNC path and the Web URL to the default location, which is the core server's \LDLogon\Patch folder.

About the Proxy settings tab

If your network uses a proxy server for external transmissions (such as Internet access), use this tab to enable and configure the proxy server settings. Internet access is required for both updating vulnerability information, and for downloading patch files from appropriate Web services.

- **Use proxy server:** Enables the proxy server option (by default, this option is off). If you enable a proxy server, you must fill in the address and port fields below.
- **Server:**
 - **Address:** Identifies the IP address of your proxy server.
 - **Port:** Identifies the port number of your proxy server.
- **HTTP based Proxy:** Enables the proxy server, if it's an HTTP-based proxy (such as Squid), so that it will successfully connect to and download patches from FTP sites. (Patches hosted at some FTP sites cannot be downloaded through an HTTP-based proxy unless you first enable this option.)
- **Requires login:** Allows you to enter a username and password if the proxy server is credentialed instead of a transparent proxy server.
 - **Username:** Enter a valid username with authentication credentials to the proxy server.
 - **Password:** Enter the user's password.

About the Alerting tab

Use this tab to configure security alerting. If you've added security definitions to the Alert group, Security and Patch Manager will alert you whenever any of those definitions is detected on any scanned device.

- **Minimum alert interval:** Specifies the shortest time interval (in minutes or hours) in which alerts for detected vulnerabilities are sent. You can use this setting if you don't want to be alerted too frequently. Set the value to zero if you want instant, real-time alerting to occur.
- **Add to Alert group:** Indicates which vulnerabilities, by severity level, are automatically placed in the Alert group during a content download process. Any definition placed in the Alert group is also automatically placed in the Scan group by default (in order to include those definitions in a security scan task).

About the Definition properties dialog

Use this dialog to view properties for downloaded content definition types, including vulnerabilities, spyware, security threats, software updates, etc. You also use this page to create your own custom definitions.

This information is read-only for downloaded definitions. For custom definitions, the fields on this dialog are editable. You can enter identification, attribute, and detection rule details information for a custom definition by using the available fields on this dialog and on the detection rule properties dialog. For more information, see [Creating custom definitions and detection rules](#).

You can use the left and right arrow buttons (<, >) to view property information for the previous or next definition in the order they are currently listed in the main window.

The Definition properties dialog contains the following tabs:

- About the General tab
- About the Description tab
- About the Dependencies tab
- About the Custom Variables tab

About the General tab

- **ID:** Identifies the selected definition with a unique, vendor-defined alphanumeric code (or user-defined in the case of a custom definition).
- **Type:** Identifies the selected item as a vulnerability, security threat, custom definition, etc.
- **Publish Date:** Indicates the date the selected definition was published by the vendor (or created by a user).
- **Title:** Describes the nature or target of the selected definition in a brief text string.
- **Severity:** Indicates the severity level of the definition. For downloaded content, this severity level is assigned by the vendor. For a custom definition, the severity is assigned by whoever created the definition. Possible severity levels include: Service Pack, Critical, High, Medium, Low, Not Applicable, and Unknown. Use this information to evaluate the risk posed by the definition, and how urgent scanning and remediation are for your network.
- **Status:** Indicates the status of the definition in the Security and Patch Manager window. The three status indicators are: Scan, meaning the selected item is enabled for the next security scan; Don't Scan, meaning it won't be scanned; and Unassigned, meaning it is in a temporary holding area and won't be scanned. For more information about these three states/groups, see [Understanding the Security and Patch Manager window](#).
- **Language:** Indicates the language of the platform identified by the definition. For custom definitions, INTL is the default value meaning the definition is language independent, and can't be edited.
- **Category:** Indicates a more specific category within an individual security content type (see above).
- **Detection Rules:** Lists the detection rules associated with the selected definition. Note that **Downloaded** indicates whether associated patch files are downloaded to the local repository, and **Silent Install** indicates whether the patch installs without user interaction.

You can right-click a detection rule to download its associated patch (or patches), disable/enable the detection rule for security scanning, uninstall its associated patches, or view its properties. You can also double-click a detection rule to view its properties.

If you're working with a custom definition, click **Add** to create a new detection rule; click **Edit** to modify the selected rule; or click **Delete** to remove the selected rule. For more information on custom definitions, see [Creating a custom detection rule](#).

About the Description tab

- **Description:** Provides additional details about the selected definition. This information is provided by vendor research and test notes (or by the user who created the custom definition).
- **More information at:** Provides a HTTP link to a vendor-specific (or user-defined) Web page, typically a support site, with more information about the selected definition.

About the Dependencies tab

This tab displays only if the selected definition has an associated prerequisite definition, or if another definition depends on the selected definition before it can run. You can use this tab to make sure your security scan task contains all the definitions necessary to operate properly before scanning devices.

A dependency relationship can exist only for the following security definition types:

- **Prerequisites:** Lists any definitions that have to be run BEFORE the selected definition can be checked for on devices. If any of the definitions in this list aren't included in your scan task, the selected definition won't be detected by the security scanner.
- **Dependencies:** Lists any definitions that won't be detected by the security scanner until AFTER the selected definition is run. Note that the selected definition will be scanned for even if these definitions aren't included in your security scan task. However, if you want your scan task to successfully detect a definition in this list, the selected definition must be run first.

About the Custom Variables tab

This tab displays only if the selected definition includes settings or values that can be modified. For example, some system configuration security threat definitions have variable settings that you can change before including them in a security scan. Also, antivirus definitions have variable settings.

Every security definition with customizable variables has a unique set of specific values that can be modified, but the Custom Variables tab will show the following information:

- **Name:** Identifies the custom variable. The name can't be modified.
- **Value:** Indicates the current value of the custom variable. Unless the variable is read-only, you can double-click this field to change the value.
- **Description:** Provides more information about the custom variable.
- **Default value:** Provides the default value is you've changed the setting and want to restore it to its original value.

To change a custom variable, double-click the **Value** field, and either select a value if there's an available drop-down list, or manually edit the value, and then click **Apply**. Note that some variables are read-only and can't be edited (indicated in the description).

About the Download associated patches dialog

Use this dialog to download patch executable files that are required to remediate the selected vulnerability but that are not currently available on the core server (or in some other specified patch repository location). Required patches must reside in the designated patch location in order for a managed device with a detected vulnerability to be remediated successfully.

- **Name:** Indicates the name of the patch executable file.
- **Definitions:** Indicates the vulnerability which is associated with this patch file.
- **Downloaded:** Shows whether the patch file has been downloaded or not.
- **Can download:** Indicates whether the patch can be automatically downloaded, or whether it has to be downloaded by a Security and Patch Manager process.
- **Show currently required patches only:** Displays only those patch files that are required to remediate the selected vulnerability at this time. In other words, the list will include patches that have superseded earlier patches, not the earlier patches.
- **Show all associated patches:** Displays a comprehensive listing of all of the associated patches for the selected vulnerability, whether they have been superseded or not.
- **Download:** Click to download the patch files from the update source site.
- **Cancel:** Cancels the download operation.

About the Detection rule properties dialog

Use this dialog to view detection rule properties for downloaded security content, or to create and edit custom detection rules.

This information is read-only for detection rules belonging to downloaded definitions. For custom definitions, the fields on the pages of this dialog are editable. You can specify detection rule settings and configure the options on each page in order to create custom detection rules. Furthermore, if the custom detection rule allows remediation, you can add special commands that run during remediation (patch install or uninstall).

You can use the left and right arrow buttons (<, >) to view property information for the previous or next detection rule in the order they are currently listed in the main window.

The Detection rule properties dialog contains the following pages:

- About the Detection rule: General information page
- About the Detection logic: Affected platforms page
- About the Detection logic: Affected products page
- About the Detection logic: Files page
- About the Detection logic: Registry settings page
- About the Detection logic: Custom script page
- About the Patch information page
- About the Detecting the patch: Files page
- About the Detecting the patch: Registry settings page
- About the Patch install commands page
- About the Patch uninstall commands page

About the Detection rule: General information page

- **Name:** Displays the name of the detection rule.
- **State:** Indicates whether the detection rule is set to scan or not to scan. These two states correspond to the Scan and Don't Scan groups (under Detection Rules) in the Security and Patch Manager window.
- **ID:** Shows the ID of the definition associates with this rule.
- **Title:** Shows the title of the definition associated with this rule.
- **Description:** Shows the description of the definition associated with this rule.
- **Comments:** Provides additional information from the vendor, if available. If you're creating or editing a custom definition, you can enter your own comments.

Detection logic pages

The following pages refer to the detection logic used by the selected detection rule to determine whether the vulnerability definition (or other definition type) exists on a scanned device.

About the Affected platforms page

Identifies the operating systems the security and patch scanner will run on to check for this rule's associated definition. In other words, only devices matching the selected platforms will attempt to process this rule. At least one platform **MUST** be selected. If a target device is running a different operating system, the security scanner quits.

About the Affected products page

- **Products:** Lists the products you want to check for with the detection rule to determine whether the associated definition exists on scanned devices.. Select a product in the list to view its name, vendor, and version information. You do not need to have a product associated with a detection rule. Associated products act as a filter during the security scan process. If none of the specified associated products are found on the device, the security scan quits. However, if no products are specified, the scan proceeds to the files check.

If you're creating or editing a custom detection rule, click **Edit** to open a new dialog that lets you add and remove products in the list. The list of available products is determined by the security and patch content you've updated via the LANDesk Security service.

- **Name:** Provides the name of the selected product.
- **Vendor:** Provides the name of the vendor.
- **Version:** Provides the version number of the selected product.

About the Files page

- **Files:** Lists the file conditions (existence, version, date, size, etc.) that are used to determine whether the associated definition exists on scanned devices. Select a file in the list to view its verification method and expected parameters. If all the file conditions are met, the device is not affected. Said another way, if any of these file conditions are **NOT** met, the vulnerability is determined to exist on that device. If there are no file conditions in the list, the scan proceeds to the registry check.

If you're creating or editing a custom detection rule, click **Add** to make the fields editable, allowing you to configure a new file condition and expected values/parameters. A rule can include one or more file conditions, depending on how complex you want to make it. To save a file condition, click **Update**. To delete a file condition from the list, select it and click **Remove**.

- **Verify using:** Indicates the method used to verify whether the prescribed file condition is met on scanned devices. For example, a detection rule can scan for file existence, version, date, size, and so on. The expected parameters that appear below the verification method are determined by the method itself (see the list below).

If you're creating or editing a custom detection rule, select the verification method from the **Verify using** drop-down list. As stated above, the parameter fields are different for each verification method, as described in the following list:

Note that the **Search for file recursively** option applies to all the file verification methods except for the MSI methods, and causes the scan to search for files in the specified path location and any existing subfolders.

- **File Existence Only:** Verifies by scanning for the specified file. Parameters are: Path (location of the file on the hard drive, including the filename), and Requirement (must exist or must not exist).
- **File Version:** Verifies by scanning for the specified file and its version number. Parameters are: Path, Minimum Version, and Requirement (must exist, must not exist, or may exist).

Note that for the File Version, Date, and Size parameters, after specifying the file path and name, you can click the **Gather Data** button to automatically populate the appropriate value fields.

- **File Date:** Verifies by scanning for the specified file and its date. Parameters are: Path, Minimum Date, and Requirement (must exist, must not exist, or may exist).
- **File Size and/or Checksum:** Verifies by scanning for the specified file and its size or checksum value. Parameters are: Path, Checksum, File size, and Requirement (must exist, must not exist, or may exist).
- **MSI Product ID installed:** Verifies by scanning to ensure the specified MSI product is installed (a product installed by the Microsoft Installer utility). Parameters are: Guid (the product's global unique identifier).
- **MSI Product ID NOT installed:** Verifies by scanning to ensure the specified MSI product isn't installed. Parameters are: Guid.

About the Registry settings page

- **Registry:** Lists the registry key conditions that are used to determine whether the associated vulnerability (or other type) exists on a scanned device. Select a registry key in the list to view its expected parameters. If any of these conditions are NOT met, the vulnerability is determined to exist on that device.

Important: If there are no registry conditions in the list, AND there were no file conditions on the Files tab, the scan fails. In other words, a detection rule must have at least one file or registry condition.

If you're creating or editing a custom detection rule, click **Add** to make the fields editable allowing you to configure a new registry key condition and expected parameters. A rule can include one or more registry conditions. To save a registry condition, click **Update**. To delete a registry condition from the list, select it and click **Remove**.

- **Key:** Identifies the registry key's expected folder and path.
- **Name:** Identifies the expected name of the key.
- **Value:** Identifies the expected value of the key.
- **Requirement:** Indicates whether the registry key must or must not exist on target devices.

About the Custom script page

Use this page if you want to write a custom VB script that checks for any other conditions on scanned devices. The security scanner agent's runtime properties that can be accessed with a custom script to report its results are: Detected, Reason, Expected, and Found.

About the Patch information page

Use this page to define and configure the rule's associated patch file (if one is required for remediation) and the logic used to detect whether the patch is already installed. You can also configure additional patch file install or uninstall commands for customized remediation.

This page and the ones under it refer to the patch file required to remediate a vulnerability. These pages are applicable only if the selected detection rule allows remediation by deploying a patch file. If the detection rule is limited to scanning only, or if the security content type doesn't use patch files for remediation, as in the case of security threats, or spyware, then these pages are not relevant.

- **Repaired by patch, or detection only:** Click one of these options to specify whether the detection rule will just check for the presence of the associated definition (detect only), or if it can also remediate that definition by deploying and installing the required patch.
- **Patch download information:**
 - **Patch URL:** Displays the full path and file name of the patch file required to remediate the selected definition if detected. The is location from where the patch file is downloaded.
 - **Auto-downloadable:** Indicates whether the patch file can be automatically downloaded from its hosting server. You can use this option with custom detection rules if you want to prevent patch files from being downloaded via the rule's shortcut menu. For example, you may need to prevent automatic patch download if there's a firewall that blocks access to the hosting server.
 - **Download:** If you're creating or editing a custom detection rule that performs remediation, and you've entered a patch filename and URL, you can click **Download** to attempt to download the patch file at this time. You can download the patch file at a later time if you prefer.
- **Repair information:**
 - **Unique filename:** Identifies the unique executable filename of the patch file.

It is strongly recommended that when you download a patch file, you create a hash for the patch file by clicking **Generate MD5 Hash**. (Most, if not all, known vulnerability's associated patch files should have a hash.) The patch file must be downloaded before you can create a hash. A hash file is used to ensure the integrity of the patch file during remediation (i.e., when it's deployed and installed on an affected device). The security scanner does this by comparing the hash code created when you click the Generate MD5 Hash button with a new hash it generated immediately before attempting to install the patch file from the patch repository. If the two hash files match, remediation proceeds. If the two hash files do not match, indicating the patch file has changed in some way since being downloaded to the repository, the remediation process quits.

- **Requires reboot:** Indicates whether the patch file requires a device reboot before completing its installation and configuration processes on the device.
- **Silent install:** Indicates whether the patch file can complete its installation without any end user interaction.

Detecting the patch pages

The following pages refer to the detection logic used by the rule to check if the patch is already installed on devices.

Important: ALL of the specified conditions for BOTH files and registry settings must be met in order for the patch file to be detected as installed on a device.

About the Files page

This page specifies the file conditions used to determine whether the patch file is already installed on a device. The options on this page are the same as on the Files page for definition detection logic (see above). However, the logic works conversely when detecting patch installation. In other words, when checking for a patch installation, all of the file conditions specified on this page must be met in order to determine an installation.

About the Registry settings page

This page specifies the registry key conditions used to determine whether the patch file is already installed on a device. The options on this page are the same as on the Registry settings page for definition detection logic (see above). However, the logic works conversely in this case. In other words, when checking for a patch installation, all of the registry conditions specified on this page must be met in order to determine an installation.

Important: ALL of the specified conditions for BOTH files and registry settings must be met in order for the patch file to be detected as installed on a device.

Patch installation and removal pages

The following pages let you configure additional commands that run when the patch is installed on or uninstalled from affected devices.

This option is available only for custom definitions that allow remediation.

These commands are useful if you need to program specific actions on target devices to ensure successful remediation. Additional commands aren't required. If you don't configure any additional commands, the patch file executes by itself by default. Keep in mind that if you do configure one or more additional commands, you must also include a command that executes the actual patch file with the Execute command.

About the Patch install commands page

Use this page to configure additional commands for a patch install task. The available commands are the same for patch install and uninstall.

- **Commands:** Lists commands in the order they will run on target devices. Select a command to view its arguments. You can change the order of commands with the **Move Up** and **Move Down** buttons. To remove a command from the list, select it and click **Remove**.
- **Add:** Opens a dialog that lets you select a command type to add to the Commands list.
- **Command Arguments:** Displays the arguments that define the selected command. An argument's values can be edited. To edit any argument, double-click its **Value** field, and then type directly in the field. For all the command types, you can also right-click in the **Value** field to insert a macro/variable into the argument.

The following list describes the commands and their arguments:

- **Copy:** Copies a file from the specified source to the specified destination on the hard drive of the target device. This command can be used before and/or after executing the patch file itself. For example, after extracting the contents of a compressed file with the Unzip command, you may want to copy files from one location to another.

The arguments for the Copy command are: Dest (full path where you want to copy the file, not including the filename) and Source (full path, and file name, of the file you want to copy).

- **Execute:** Runs the patch file, or any other executable file, on target devices.

The arguments for the Execute command are: Path (full path, and file name, where the executable file resides; for the patch file, you can use the %SDMCACHE% and %PATCHFILENAME% variables), Args (command-line options for the executable file; note this field is not required), Timeout (number of seconds to wait for the executable to terminate before continuing to the next command in the list, if the Wait argument is set to true), and Wait (true or false value that determines whether to wait for the executable to terminate before continuing to the next command in the list).

- **ButtonClick:** Automatically clicks a specified button that displays when an executable file runs. You can use this command to program a button click if such interaction is required by the executable.

In order for the ButtonClick command to work properly, the Wait argument for the preceding Execute command must be set to false so that the executable doesn't have to terminate before continuing to the button click action.

The arguments for the ButtonClick command are: Required (true or false value indicating whether the button must be clicked before proceeding; if you select true and the button can't be clicked for any reason, remediation quits; if you select false and the button can't be clicked, remediation will continue), ButtonIDorCaption (identifies the button you want clicked by its text label, or its control ID), Timeout (number of seconds it takes for the button you want clicked appears when the executable runs), and WindowCaption (identifies the window or dialog where the button you want clicked is located).

- **ReplaceInFile:** Edits a text-based file on target devices. Use this command if you need to make any modifications to a text-based file, such as a specific value in an .INI file, before or after executing the patch file to ensure that it runs correctly.

The arguments for the ReplaceInFile command are: Filename (full path and name of the file you want to edit), ReplaceWith (exact text string you want to add to the file), and Original Text (exact text string you want to replace in the file).

- **StartService:** Starts a service on target devices. Use this command to start a service required for the patch file to run, or to restart a service that was required to be stopped in order for the patch file to run.

The arguments for the StartService command are: Service (name of the service).

- **StopService:** Stops a service on target devices. Use this command if a service must be stopped on a device before the patch file can be installed.

The arguments for the StopService command are: Service (name of the service).

- **Unzip:** Unzips a compressed file on target devices. For example, you can use this command if remediation requires more than one file be run or copied on target devices.

The arguments for the Unzip command are: Dest (full path to where you want to extract a compressed file's contents on a device's hard drive), and Source (full path and filename of the compressed file).

- **WriteRegistryValue:** Writes a value to the registry.

The arguments for the WriteRegistryValue are: Key, Type, ValueName, ValueData, WritelfDataEmpty

About the Patch uninstall commands page

Use this page to configure additional commands for a patch uninstall task. The available commands are the same for patch install and uninstall. However, the Patch uninstall commands page includes two unique options:

- **Patch can be uninstalled:** Indicates whether the patch file can be uninstalled from remediated devices.
- **Original patch is required for uninstall:** Indicates whether the original patch executable file itself must be accessible on the core server in order to uninstall it from scanned devices.

For information on the commands, see About the Patch install command page above.

About the Purge security and patch definitions dialog

Use this dialog to completely remove definitions (and their associated detection rules) and patches, from the core database. You may want to remove definitions if they have become obsolete, are not working properly, or if the related security risk has been totally resolved.

- **Platforms:** Specifies the platforms whose definitions you want to remove from the database.

If a definition is associated with more than one platform, you must select all of its associated platforms in order for the definition and its detection rule information to be removed.

- **Languages:** Specifies the language versions of the selected platforms whose definitions you want to remove from the database.

If you've selected a Windows or Macintosh platform, you should specify the languages whose definition information you want to remove. If you've selected a UNIX or Linux platform, you must specify the Language neutral option in order to remove those platform's language independent definition information.

- **Types:** Specifies the content types whose definitions you want to remove.

- **Purge:** Completely removes definition and detection rule information, and associated patches, for the types you've selected that belong to the specified platforms and languages you've selected. This information can only be restored by downloading the content again.
- **Close:** Closes the dialog without saving changes and without removing definition information.

About the Create security scan task dialog

Use this dialog to create and configure a task that runs the security and patch scanner on target devices. This dialog contains the following options:

- **Task name:** Enter a unique name to identify the security and patch scan task.
- **Create a scheduled task:** Adds the security and patch scan task to the Scheduled tasks window, where you can configure its scheduling and recurrence options, and assign target devices.
- **Create a policy:** Adds the security and patch scan task as a policy to the Scheduled tasks window, where you can configure the policy options.
- **Scan and repair settings:** Specifies scan and repair settings used for the scan task. Scan and repair settings determine whether the security and patch scanner displays on devices while running, reboot options, user interaction, and the content types scanned. Select a scan and repair setting from the drop-down list to assign it to the security scan task you're creating. You can click **Edit** to modify the options for the selected scan and repair setting. You can also click **Configure** to create a new scan and repair setting. For more information, see About the Configure scan and repair settings dialog.

About the Configure scan and repair settings dialog

Use this dialog to manage your scan and repair settings. Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks.

This dialog contains the following options:

- **New:** Opens the Scan and repair settings dialog where you can configure the security scan options.
- **Edit:** Opens the Scan and repair settings dialog where you can modify the selected scan and repair setting.
- **Delete:** Removes the selected scan and repair setting.
- **Use selected:** Applies the selected scan and repair setting to the task you're configuring (scan, repair, or reboot).
- **Close:** Closes the dialog, without applying a scan and repair setting to the task.

About the Scan and repair settings dialog

Use this dialog to create and edit an scan and repair setting. Scan and repair settings determine whether the security and patch scanner displays on devices while running, reboot options, user interaction, and the content types scanned.

You can create as many scan and repair settings as you like and edit them at any time. For example, you can configure a scan and repair setting with a specific notification and reboot scenario for desktop devices, and another scan and repair setting with different reboot options for servers. Or, you can configure an scan and repair setting for Windows vulnerability scanning, and another one for spyware scanning, etc.

Once configured, you can apply scan and repair settings to security scan tasks, repair tasks, uninstall tasks, and reboot tasks.

Scan and repair settings

- **Name:** Identifies the scan and repair setting with a unique name. This name appears in the Scan and repair settings drop-down list on a security task dialog.

The Scan and repair settings dialog contains the following tabs:

- About the General tab
- About the Repair tab
- About the Reboot tab
- About the MSI tab
- About the Networking tab

About the General tab

- **Show progress when running:** Enables the security and patch scanner to display information on end user devices while it is running. Click this option if you want to show scanner activity, and if you want to configure other display and interaction options in this dialog. If you don't click this option, none of the other tabs on this dialog are available to configure, and the scanner runs transparently on devices.
- **Allow user to cancel scan:** Shows a Cancel button on the Security and Patch Manager dialog on the end user device. Click this option if you want the end user to have the opportunity to cancel a scan operation. If this option is not checked, the dialog doesn't have a Cancel button and the end user can't stop the scan.
- **When no reboot is required:**
 - **Require end user input before closing:** For a scan or repair task that doesn't require a reboot in order to complete its full operation, click this option if you want the scanner to prompt the end user before its display dialog closes on the device. If you select this option, and the end user does not respond the dialog remains open which could cause other scheduled tasks to timeout.
 - **Close after timeout:** For a scan or repair task that doesn't require a reboot, click this option if you want the scanner's display dialog to close after the duration you specify.
- **Scan for:** Specifies which content types you want to scan for with this scan task. You can select either a custom group (preconfigured) or specific content types. You can select only those content types for which you have a LANDesk Security Suite content subscription. Also, the actual security definitions that are scanned for depends on the contents of the Scan group in the Security and Patch Manager window. In other words, if you select vulnerabilities and security threats in this dialog, only those vulnerabilities and security threats currently residing in their respective Scan groups will be scanned for.
- **Enable autofix:** Indicates that the security and patch scanner will automatically deploy and install the necessary associated patch files for any vulnerabilities or custom definitions it detects on scanned devices. This option applies to security scan tasks only. In order for autofix to work, the patch file must also have autofix enabled.

About the Repair tab

- **Prompt user before repairing, installing or uninstalling a patch:** Click this option if you want a prompt to appear on the end user device, with message and interaction controls as configured with the options below. If you don't click this option, the operation will proceed automatically without prompting the end user.
- **Allow user to cancel before starting repair, install or uninstall:** Click this option if you want the end user to have the opportunity to cancel a patch file repair operation.
- **Message:** Type a message in this box that will appear in the security and patch scanner's display dialog on the end user device WHEN a security scan task detects any of the specified definitions on the scanned device. You can customize this message depending on the type of security scan you're running.
- **If no end user response:**
 - **Wait for user response:** For a patch file operation prompt that doesn't receive a response, click this option if you want the scanner to continue waiting indefinitely.
 - **After timeout, automatically:** For a patch file operation prompt that doesn't receive a response, click this option if you want the scanner to automatically proceed and perform the patch file operation or close without performing the operation, after the duration you specify.
- **Maximum percent of bandwidth to use when downloading:** Specify the bandwidth percentage you want to be used for the patch file download from the patch repository to scanned devices. You can use this setting to balance network traffic for large patch file deployments.

About the Reboot tab

- **When deciding whether to reboot:** Specify how you want the security and patch scanner to act when a scan or repair task tries to reboot a device for any reason. You can select for the device to never reboot, reboot only if needed, or always reboot.
- **When rebooting:**
 - **Prompt user before rebooting:** For when a reboot occurs, click this option if you want the security and patch scanner to prompt the end user. If you select this option, you can configure the accompanying reboot options below.
 - **Allow user to defer reboot:** Shows a defer button on the reboot prompt on the end user device. Specify the deferral time span and the number of times the end user can defer the reboot. The deferral (or snooze) time begins with the next local scheduler poll.
 - **Allow user to cancel reboot:** Shows a cancel button on the reboot prompt on the end user device.
 - **Reboot message:** Type a message in this box that will appear in the security and patch scanner's display dialog on the end user device WHEN a security scan task prompts the end user before attempting to reboot the device.
 - **Wait for user response:** For a reboot prompt that doesn't receive a response, click this option if you want the scanner to continue waiting indefinitely. If there's no response, the prompt remains open.
 - **After timeout, automatically:** For a reboot prompt that doesn't receive a response, click this option if you want the scanner to automatically proceed and either reboot, snooze, or close the prompt without rebooting, after the duration you specify.

About the MSI tab

Use this tab if a patch file needs to access its originating product installation resource in order to install any necessary supplemental files. For example, you may need to provide this information when you're attempting to apply a patch for Microsoft Office or some other product suite.

- **Original package location:** Enter the UNC path to the product image.
- **Credentials:** Enter a valid user name and password to authenticate to the network share specified above.

About the Networking tab

Use this tab to identify an alternate core server that can be used for security scanning and remediation if the main core server is not available.

- **Communicate with alternate server:** Enables communication with an alternate server.
- **Servename:** Enter the name of a valid, licensed LANDesk core server.

Note: The syntax for the servename field should be: <servename>:<port number> where port number is the secure port 443 for SSL transmission. If you enter only a servename, without specifying port 443, it defaults to port 80 which is the standard HTTP port.

About the Security and patch information dialog

Use this dialog to view detailed security and patch information for selected devices, such as scan results, detected definitions, missing and installed patches (or software updates), and repair history. Use the **Clear** button to remove all scan information from the database for the selected devices.

You can right-click a vulnerability (or other content type) in this view and directly create a repair task, or enable/disable the autofix option for applicable types.

Displayed information is based on the selected type

The group names and information fields that display on this page are dynamic, depending on the security content type you select from the Type drop-down list. For example, if you select vulnerabilities, the following information fields display:

- **Missing Patches (Vulnerabilities Detected):** Lists all of the vulnerabilities detected on the device by the last scan.
- **Installed Patches:** Lists all of the patches installed on the device.
- **Repair History:** Shows information about the remediation tasks attempted on the device. This information is helpful when troubleshooting devices. To clear this data, click **Purge Repair History**, specify the devices and time range settings, and then click **Purge**.
- **Vulnerability Information:**
 - **Title:** Displays the title of the selected vulnerability.
 - **Detected:** Indicates whether the selected vulnerability was detected.
 - **First detected:** Displays the date and time the vulnerability was initially detected on the device. This information can be useful if you've performed multiple scans.
 - **Reason:** Describes the reason why the selected vulnerability was detected. This information can be useful in helping you decide whether the security risk is serious enough to prompt immediate remediation.

- **Expected:** Displays the version number of the file or registry key the vulnerability scanner is looking for. If the version number of the file or registry key found on the scanned device matches this number, the vulnerability does not exist.
- **Found:** Displays the version number of the file or registry key found on the scanned device. If this number is different than the Expected number above, the vulnerability exists.
- **Patch Information:**
 - **Patch Required:** Displays the file name of the patch executable required to remediate the selected vulnerability.
 - **Patch Installed:** Indicates whether the patch file has been installed.
 - **Last action date:** Displays the date and time the patch was installed on the device.
 - **Action:** Indicates whether the last action was an install or an uninstall.
 - **Details:** Indicates whether the deployment/installation was successful. If an installation failed, you must clear this status information before attempting to install the patch again.
 - **Clear:** Clears the current patch installation date and status information for the selected device. Clearing this information is necessary in order to attempt to deploy and install the patch again.

About the Schedule repair dialog

Use this dialog to create and configure a repair task for the following definition types: vulnerabilities, spyware, LANDesk software updates, custom definitions, and security threats (if they have patch). The schedule repair option is not applicable to blocked applications.

This dialog includes the following two tabs:

General tab

- **Task name:** Identifies the repair task with a unique name. The default is the name of the selected definition or the custom group. You can edit this name if you prefer.
- **Repair as a scheduled task:** Creates a security repair task in the Scheduled tasks window when you click **OK**.
- **Split into staging task and repair task:** (Optional) Allows you to create to separate tasks in the Scheduled tasks tool; one task for staging the required patch files in the target device's local cache; and one task for actually installing those patch files on the affected devices.
 - **Select computers to repair:** Specifies which devices to add to the scheduled repair task. You can choose no devices, all affected devices (devices where the definition was detected by the last security scan), or only the affected devices that are also selected (this last option is available only when you access the Schedule repair dialog from within a device Security and patch information dialog).
 - **Use Multicast:** Enables Targeted Multicast for patch deployment to devices. Click this option, and click **Multicast Options** if you want to configure multicast options. For more information, see About the Multicast Options dialog.
- **Repair as a policy:** Creates a security repair policy when you click **OK**.
 - **Add query representing affected devices:** Creates a new query, based on the selected definition, and applies it to the policy. This query-based policy will search for devices affected by the selected definition, and deploy the associated patch.

- **Download patch only from local peers:** Restricts patch deployment so that it will only take place if the patch file is located in the device local cache or on a peer on the same subnet. This option conserves network bandwidth, but note that for the patch installation to be successful, the patch file must currently reside in one of these two places.
- **Download patch only (Do not repair):** Downloads the patch file to the patch repository but does not deploy the patch. You can use this option if you want to retrieve the patch file in a staging scenario for testing purposes before actual deployment.
- **Scan and repair settings:** Specifies which scan and repair setting is used for the repair task to determine whether the security and patch scanner displays on devices when it is running. Select an scan and repair setting from the drop-down list, or click **Configure** to create a new scan and repair setting.

Patches tab

Use this tab to show either required patches only or all associated patches for the selected vulnerability. The fields on this page are the same as the fields on the Download associated patches dialog.

You can also download patches from this tab, if they have not already been placed in the patch repository (click **Download**).

About the Multicast options dialog

Use this dialog to configure the following Targeted Multicast options for a scheduled security repair task:

- **Multicast Domain Discovery:**
 - **Use multicast domain discovery:** Select this option if you want Targeted Multicast to do a domain discovery for this job. This option won't save the domain discovery results for reuse.
 - **Use multicast domain discovery and save results:** Select this option if you want Targeted Multicast to do a domain discovery for this job and save the results for future use, saving time on subsequent multicasts.
 - **Use results of last multicast domain discovery:** Use this option once you've had Targeted Multicast do a domain discovery that saved the results.
- **Have domain representative wake up computers:** Use this option if you want computers that support Wake On LAN technology to turn on so they can receive the multicast.
- **Number of seconds to wait after Wake on LAN:** How long domain representatives wait to multicast after the Wake On LAN packet has been sent. The default waiting period is 120 seconds. If some computers on your network take longer than 120 seconds to boot, you should increase this value. The maximum value allowed is 3600 seconds (one hour).

The options below let you configure task-specific Targeted Multicast parameters. The defaults should be fine for most multicasts. Here are what the options do:

- **Maximum number of multicast domain representatives working simultaneously:** No more than this number of representatives will be actively doing a multicast at one time.

- **Limit the processing of machines that failed multicast:** When a device fails to receive the file through multicast, it will download the file from the Web or file server. This parameter can be used to limit the number of devices that will obtain the file at one time. For example, if the maximum number of threads was 200 and the maximum number of multicast failure threads was 20, the Custom Job dialog would process no more than 20 computers at a time that failed the multicast. The Custom Job dialog will process up to 200 devices at a time if they successfully received the multicast, but no more than 20 of the 200 threads will be processing devices that failed the multicast task. If this value is set to 0, the Custom Job dialog won't perform the distribution portion of the task for any computer that failed multicast.
- **Number of days the files stay in the cache:** Amount of time that the file being multicast can stay in the cache on each target computer. After this period of time, the file will be automatically purged.
- **Number of days the files stay in multicast domain representative cache:** Amount of time that the file being multicast can stay in the cache on the multicast domain representative. After this period of time, the file will be automatically purged.
- **Minimum number of milliseconds between packet transmissions (WAN or Local):** Minimum amount of time to wait between sending out multicast packets.

This value is only used when the domain representative isn't multicasting a file from its own cache. If this parameter isn't specified, then the default minimum sleep time stored on the subnet/domain representative computer will be used. You can use this parameter to limit bandwidth usage across the WAN.

- **Maximum number of milliseconds between packet transmissions (WAN or Local):** Maximum amount of time to wait between sending out multicast packets. For more information, see Minimum number of milliseconds between packet transmissions above.

About the Uninstall patch dialog

Use this dialog to create and configure an uninstall task for patches that have been deployed to affected devices.

- **Task name:** Identifies the task with a unique name. The default is the name of the patch. You can edit this name if you prefer.
- **Uninstall as a scheduled task:** Creates an uninstall patch task in the Scheduled tasks window when you click **OK**.
 - **Select targets:** Specifies which devices to add to the uninstall patch task. You can choose no devices, all devices with the patch installed, or only the devices with the patch installed that are also selected (this last option is available only when you access the Uninstall Patch dialog from within a device Security and Patch Information dialog).
- **If the original patch is required:**
 - **Use Multicast:** Enables Targeted Multicast for deploying the uninstall patch task to devices. Click this option, and click **Multicast Options** if you want to configure the multicast options. For more information, see About the Multicast Options dialog below.
- **Uninstall as a policy:** Creates an uninstall patch policy in the Scheduled tasks window when you click **OK**.
 - **Add query representing affected devices:** Creates a new query, based on the selected patch, and applies it to the policy. This query-based policy will search for devices with the selected path installed and uninstall it.

- **Scan and repair settings:** Specifies which scan and repair setting is used for the uninstall task to determine whether the security and patch scanner displays on devices, reboot options, MSI location information, etc. Select an scan and repair setting from the drop-down list, or click **Configure** to create a new scan and repair setting.

About the Create reboot task dialog

Use this dialog to create and configure a generic reboot task. A reboot task can be useful when you want to install patches (without rebooting) as a single process and then reboot those remediated devices as another separate task. For example, you can run a scan or a patch install task during the day, and then deploy a reboot only task at a more convenient time for end users.

- **Task name:** Identifies the task with a unique name.
- **Create a scheduled task:** Creates a reboot task in the Scheduled tasks window when you click **OK**.
- **Create a policy:** Creates a reboot policy when you click **OK**.
- **Scan and repair settings:** Specifies which scan and repair setting is used for the task to determine whether the security and patch scanner displays on devices when it is running. Select an scan and repair setting from the drop-down list, or click **Configure** to create a new scan and repair setting.

About the Configure firewall settings dialog

Use this dialog to configure the firewall settings you want to check for (and modify) with the editable custom variables that are available for the Configure the Windows firewall security threat. (This specific security threat's ID is: ST000102.)

- **Current exceptions:**
- **Add program:**
- **Add port:**
- **Edit:**
- **Delete:**
- **OK:**
- **Cancel:**

About the Change scope dialog

This dialog is accessed from the **Configure firewall** dialog (double-click the **Value** field on the **Custom variables** tab of the Configure the Windows firewall security threat's properties dialog).

You can use this dialog to configure the scope (or group) of devices that are affected by the selected exception to the firewall (whether it is a program, port, service, etc.).

- **Any computer:**
- **My network (subnet) only:**
- **Custom list:**
- **OK:**
- **Cancel:**

Macintosh help

About the OSD script dialog

Use this dialog to capture or deploy an image. The OSD script dialog consists of three configuration pages: **General**, **Image path**, and **Network**. However, only certain configuration pages are required for the different tasks.

For more information, see Operating system deployment for Macintosh devices.

General

Use this configuration page to specify the Bootp (NetBoot) server and provide a description of the script. The **General** configuration page is used for all OSD scripts.

- **Description:** Provides a unique description of the script to differentiate it from other scripts.
- **Enter the IP address of your BootP server:** Specifies the IP address of your Mac OS X server.
- **Netboot image:** Specifies the path to the image on the server.

Image path

Use this configuration page to specify the storage location of the image on the server. The **Image path** configuration page is used for the capture image and deploy image scripts.

- **Image file URL:** Specifies the scheme type and location of the image.
- **User name:** Specifies the user name for accessing the server.
- **Password:** Specifies the password for accessing the server.
- **Confirm password:** Confirms the password for accessing the server.

Network

Use this configuration page to specify the names of the devices being imaged. The **Network** configuration page is used for the deploy image scripts.

- **First attempt to get and use existing computer names from the inventory database:** Attempts to use the original name in the database for profiles being deployed to devices.
- **When necessary, use the following template to name target computers:** Specifies a generic naming convention for providing names for profiles being deployed to devices when the original is not found.

Configuring the LANDesk Management Gateway

The LANDesk Management Gateway is an Internet appliance that provides secure communication and functionality over the Internet. It acts as a meeting place where console and managed devices are connected through their Internet connections—even if they are behind firewalls or use a proxy to access the Internet.

Read this topic to learn about:

- Setting up the Management Gateway connection
- Posting the core certificate to the Management Gateway
- Managing client certificates
- Creating an on-demand remote control agent package

Setting up the Management Gateway connection

The **Gateway information** tab lets you specify and test the connection and proxy settings used by the core to connect to the Management Gateway.

To specify the connection information

1. On the **Gateway information** tab, specify the Management Gateway information.
2. If the Management Gateway uses an internal address that is different from its public address (for example, if it's located in a DMZ-type environment), check **Use separate internal address** and specify the internal name and address.
3. If the core will connect to the Management Gateway through a proxy, check **Use proxy** and specify the proxy settings.
4. Click **Test settings** to test the core server connection to the Management Gateway.
5. If the test fails, check the information you entered and correct any mistakes, then click **Test settings** to make sure the connection works.

Posting the core certificate to the Management Gateway

Before the core can connect through the Management Gateway, you must post the core certificate to it.

To post the core certificate

1. On the **Certificates** tab, click **Post to Management Gateway**.
2. Click **OK** to post the certificate.

Managing client certificates

Each managed device is required to have a valid digital certificate in order to connect through the Management Gateway. You can manage the list of devices that have been granted certificates by blocking or deleting the ability of any formerly trusted device to connect through the Management Gateway.

To block or delete connection ability

1. Select the device(s) you want to block or delete. You can use **Shift-click** or **Ctrl-click** to select multiple devices.
2. Click **Block selection** or **Delete selection**.
3. When finished, click **OK**.

To unblock connection ability

1. Uncheck the **Block** checkbox for each device you want to unblock.
2. When finished, click **OK**.

Creating an on-demand remote control agent package

You can create an on-demand remote control agent package that can be downloaded by devices that have not been configured to connect through the Management Gateway. This allows them to be remote controlled through the Management Gateway.

To create an on-demand remote control agent

1. Click the **Certificates** tab.
2. Click **Create**.
3. Specify the organization name. The device will only be viewable to administrators that belong to the same organization.
4. Click **Save**.
5. Specify the location to which you want the remote control agent to be saved.
6. Click **Save**.

After creating the remote control agent, you can distribute it on CD or post it to an accessible location for download by managed devices.

Local accounts management help

About the New user dialog

Use this dialog to create a new user. For more information, see Managing local users.

- **User name:** Specifies the user name for the new user
- **Full name:** Specifies the full name of the user.
- **Description:** Provides a description of the user
- **Password:** Specifies a password for the user to authenticate to the console.
- **Confirm password:** Confirms the password.
- **User must change password at next logon:** Causes the user to have to change their password upon initial logon into the console.
- **User cannot change password:** Disallows the users from changing the password.
- **Password never expires:** Causes the password to never expire, so the user won't have to change the password.
- **Account is disabled:** Disables the account.

About the Edit user dialog

Use this dialog to edit the user properties. The dialog consists of three configuration tabs, **General**, **Member of**, and **Profile**.

For more information, see Managing local users.

General

Use this configuration page to specify the user name, full name, and description of the user. You can also change some of the account properties.

- **User name:** Specifies the user name of the user (if available).
- **Full name:** Specifies the full name of the user.
- **Description:** Specifies the description of the user
- **User must change password at next logon:** Specifies if the user has to change their password upon logging in to the console.
- **User cannot change password:** Specifies if the user can change their password.
- **Password never expires:** Specifies if the password will expire.
- **Account is disabled:** Specifies if the account is disabled.
- **Account is locked:** Unlocks the account so the user can authenticate to the console. This option is available when the user has unsuccessfully tried to log in to their account over three times in one session.

Member of

Use this configuration page to assign the user to groups.

- **Selected groups:** Lists the groups the user is a member of.
- **Add:** Launches the **Select groups** dialog, which enables you to add the groups you want the user to be a member of.

- **Remove:** Removes the user as a member of the selected groups and removes the groups from the list.

Profile

Use this configuration page to specify the account information for the user.

- **User profile path:** Specifies the network path to the user's account and profile.
- **Logon script:** Specifies the logon scripts.
- **Local path:** Specifies a local path as the home directory.
- **Connect:** Specifies a network directory as the home directory. Select a drive and then insert the network path.

About the Group properties dialog

Use this dialog to configure the group. For more information, see [Managing local groups](#).

- **Group name:** Specifies the name of the group.
- **Description:** Provides a description of the group.
- **Members:** Lists the users that belong to the group.
- **Add:** Launches the **Select users** dialog, which enables you to add users to the group.
- **Remove:** Removes the selected users from the group.